МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Саратовский государственный технический
университет имени Гагарина Ю.А.»

Профессионально-педагогический колледж

УТВЕРЖДАЮ
Директор
Профессионально-педагогического
колледжа СГТУ имени Гагарина Ю.А.
_____ Т.И. Кузнецова
«29» апреля 2023 г.

РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

специальность

10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рабочая программа рассмотрена
на заседании цикловой методической комиссии
информационной безопасности и компьютерных систем
протокол № 10 от «09» 06 2023 г.
Председатель ЦМК _____ М.А. Ястребова

Саратов 2023

Рабочая программа Производственной практики разработана в соответствии с Федеральным государственным образовательным стандартом (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки РФ от 9 декабря 2016 года № 1553.

Группа разработчиков:

Захаров Е.В. - Ведущий инженер электросвязи, ГУСПД ОУССиИС МРЦУССиМИС, Департамент эксплуатации технической инфраструктуры БТИ МРФ «Волга» ПАО «Ростелеком»

Таланова Ю.В. - преподаватель Профессионально-педагогического колледжа СГТУ имени Гагарина Ю.А.

Рецензенты:

Внутренний: Ястребова М.А. – преподаватель высшей квалификационной категории ППК СГТУ имени Гагарина Ю.А.

Внешний: Жордочкин А.В. - генеральный директор ООО «Ирис»

СОДЕРЖАНИЕ

Стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ **4**

2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕПРАКТИКИ **7**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ **10**

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ **16**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

1.1. Область применения рабочей программы

Рабочая программа практики Производственной является частью программы подготовки специалистов среднего звена (далее - ППССЗ) в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части основных вида деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Производственная практика проводится при освоении обучающимися профессиональных компетенций в рамках профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

1.2. Место практикив структуре ППССЗ.

Производственная практика входит в Профессиональный цикл.

1.3. Цели и требования к результатам освоения практики

Производственная практика направлена на формирование у обучающихся профессиональных компетенций и общих компетенций в рамках профессионального модуля, реализуется в форме практической подготовки, организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

1.3.1. Перечень общих компетенций

Код	Наименование общих компетенций
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.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.3.2. Перечень профессиональных компетенций

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

1.3.3. В результате освоения программы практики обучающийся должен:

иметь практический опыт	- установке и настройке программных средств защиты информации; - тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; - учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности;
уметь	- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; - использовать типовые программные криптографические средства, в том числе электронную подпись; - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

1.4. Количество часов на освоение программы практики:

Всего: 144 часа.

2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

3.1. Тематический план практики

Код (ПК, ОК)	Код и наименование профессионального модуля	Количество часов практики	Наименованияразделовпрактики	Количество часов по разделам, МДК
1	2	3	4	5
ПК 2.1-2.6 ОК 01-11	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	144	Инструктаж	**6**
			МДК 02.01 Программные и программно-аппаратные средства защиты информации МДК 02.02 Криптографические средства защиты информации	**126**
			Обобщение материалов, оформление дневника и отчета по практике.	**6**
			Промежуточная аттестация в форме дифференцированного зачета	**6**

3.2. Содержание практики

Наименование разделов, тем практики	Виды работ	Объем часов	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4	5
Инструктаж	- Согласование порядка выполнения заданий с руководителем практики от базы практики. - Прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка предприятия/организации, являющейся базой практики.	6	1	ОК 01-11
Тема 1. Анализ принципов построения систем информационной защиты производственных подразделений	1. Анализ принципов построения систем информационной защиты производственных подразделений	18	3	ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 2.2
Тема 2. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.	2. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.	6	3	ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.2

Тема 3. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	3. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	18	3	ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.6
Тема 4. Обеспечение учета, обработки, хранения и передачи конфиденциальной информации	4. Обеспечение учета, обработки, хранения и передачи конфиденциальной информации	30	3	ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.4
Тема 5. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы	5. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы	42	3	ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.1 ПК 2.5
Тема 6. Диагностика, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности	6. Диагностика, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности	12	3	ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.3
Обобщение материалов, оформление дневника и отчета по практике.		6	3	ОК 01-11 ПК 1.1-1.4
Промежуточная аттестация в форме дифференцированного зачета		6	3	ОК 01-11 ПК 1.1-1.4
Всего:		***144***		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

3.1. Требования к минимальному материально-техническому обеспечению практики

Практика может проводиться в организации, осуществляющей деятельность по профилю соответствующей образовательной программы, в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки, на основании договора. Требуется создание профильной организацией условий для реализации программы практики в форме практической подготовки, предоставления оборудования и технических средств обучения в объеме, позволяющем выполнять виды работ, определенные программой практики.

Типовое оборудование, технологическое оснащение рабочих мест, технические средства обучения.

Типовое лицензионное программное обеспечение.

Учебно-наглядные пособия, имеющиеся на предприятии.

Персональные компьютеры, имеющие выход в глобальную сеть Интернет, оснащен лицензионным программным обеспечением.

3.2. Учебно-методическое и информационное обеспечение реализации практики

Нормативно-правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». - Режим доступа: http://www.consultant.ru/
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». - Режим доступа: http://www.consultant.ru/
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». - Режим доступа: http://www.consultant.ru/
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». - Режим доступа: http://www.consultant.ru/
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». - Режим доступа: http://www.consultant.ru/
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». - Режим доступа: http://www.consultant.ru/

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». - Режим доступа: http://www.consultant.ru/

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». - Режим доступа: http://www.consultant.ru/

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608. - Режим доступа: http://www.consultant.ru/

10. Приказ ФСТЭК России от 17.07.2017 N 134 (ред. от 17.12.2019) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" (Зарегистрировано в Минюсте России 09.08.2017 N 47722) - Режим доступа: http://www.consultant.ru/

11. Приказ ФСТЭК России от 12.07.2012 N 84 (ред. от 20.05.2015) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации" (Зарегистрировано в Минюсте России 20.08.2012 N 25220) - Режим доступа: http://www.consultant.ru/

12. Приказ ФАПСИ 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». - Режим доступа: http://www.consultant.ru/

13. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». - Режим доступа: http://www.consultant.ru/

14. 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. – Режим доступа: http://docs.cntd.ru/

15. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – Режим доступа: http://docs.cntd.ru/

16. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Режим доступа: http://docs.cntd.ru/

17. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – Режим доступа: http://docs.cntd.ru/

18. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Практические правила управления информационной безопасностью. – Режим доступа: http://docs.cntd.ru/

19. 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. – Режим доступа: http://docs.cntd.ru/

20. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Режим доступа: http://docs.cntd.ru/

21. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Режим доступа: http://docs.cntd.ru/

22. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Режим доступа: http://docs.cntd.ru/

23. ГОСТ 34.311-95 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (аутентичен ГОСТ Р 34.11-94). – Режим доступа: http://docs.cntd.ru/

24. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

25. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Режим доступа: http://docs.cntd.ru/

26. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

27. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Режим доступа: http://docs.cntd.ru/

28. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

29. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/

30. 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. – Режим доступа: http://docs.cntd.ru/

31. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

32. 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. – Режим доступа: http://docs.cntd.ru/

33. 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. – Режим доступа: http://docs.cntd.ru/

34. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

35. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

Основные учебные издания

36. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлинский; под ред. В.Н. Пржегорлинского. - 1-е изд. - М. : Издательский центр «Академия», 2020. – 288 с. В пер. ISBN 978-5-4468-8717-0

37. 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. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

38. 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. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

39. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности / учеб. пособие для студ. учреждений сред. проф. образования / Е.Б. Белов, В.Н. Пржегорлинский. - 2-е изд., испр. и доп. - М. : Издательский центр «Академия», 2020. – 336 с. В пер. ISBN 978-5-4468-8456-8

40. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

41. Костров Б.В. Сети и системы передачи информации : учебник/ Б.В. Костров, В.Н. Ручкин : (2-е изд.) (в электронном формате) 2019. https://academia-library.ru

42. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина; под ред. В.Н. Пржегорлинского.- 1-е изд. - М. : Издательский центр «Академия», 2019. – 272 с. В пер. ISBN 978-5-4468-8718-7

43. Бубнов А.А. Основы информационной безопасности : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, О.А. Савинкин. - 3-е изд., стер. - М. : Издательский центр «Академия», 2020. – 256 с. В пер. ISBN 978-5-4468-8682-1

Дополнительные учебные издания

44. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Режим доступа: http://www.consultant.ru/

46. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Режим доступа: http://www.consultant.ru/

47. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/

48. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/

49. 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. – Режим доступа: http://docs.cntd.ru/

50. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - Режим доступа: http://www.consultant.ru/

51. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

52. Методика определения актуальных угроз безопасности персональных

данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Режим доступа: http://www.consultant.ru/

53. 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. - Режим доступа: http://www.consultant.ru/

Интернет-ресурсы

54. Сайт журнала Информационная безопасность - Режим доступа: http://www.itsec.ru

55. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/

56. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/

57. Федеральный портал. Российское образование. - Режим доступа:http://www.edu.ru

Методические указания по выполнению заданий практики

58. Методические указания по выполнению заданий практики.

3.3. Общие требования к организации образовательного процесса

Образовательная деятельность при освоении профессионального модуля организуется в форме практической подготовки путем проведении практики, предусматривающей непосредственное выполнение обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Производственная практика проводится при освоении обучающимися профессиональных компетенций в рамках профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами и реализуется концентрированно, в рамках профессионального модуля. Производственная практика реализуется в профильных организациях, в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки.

Производственная практика ПП 02.01 реализуется в 8 семестре на 4 курсе (на базе 11 классов – 6 семестре, 3 курс) (в соответствии с учебным планом) после изучения МДК 02.01 Программные и программно-аппаратные средства защиты информации, МДК 02.02 Криптографические средства защиты информации.

3.4. Кадровое обеспечение образовательного процесса

Для реализации программы Производственной практики назначается ответственное лицо, соответствующее требованиям трудового законодательства Российской Федерации о допуске к педагогической деятельности, из числа работников Профильной организации.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ

4.1. Критерии оценки, формы и методы контроля и оценки результатов обучения

Код, наименование профессиональных компетенций	Критерии оценки	Формы и методы контроля и оценки результатов обучения
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	- установка и настройка программных средств защиты информации; - применение программных и программно-аппаратных средств защиты информации;	**Текущий контроль:** собеседование по результатам выполненной работы, наблюдение за процессом выполнения заданий. выполнение письменной работы "Отчет по практике") **Промежуточная аттестация**: отчет по практике.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	- установка и настройка программных средств защиты информации; - установка и настройка средства антивирусной защиты в соответствии с предъявляемыми требованиями;	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	- тестирование функций программно-аппаратных средств защиты информации; - диагностика программных и программно-аппаратных средств защиты информации; - устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	- хранение и передача информации, для которой установлен режим конфиденциальности; - проверка выполнения требований по защите информации от несанкционированного доступа	

	при аттестации объектов информатизации по требованиям безопасности информации; - использование типовых программных криптографических средств, в том числе электронной подписи;	
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	- учет, обработка, хранение и передача информации, для которой установлен режим конфиденциальности; - установка, настройка, применение программных и программно-аппаратных средств защиты информации;	
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	- осуществление мониторинга и регистрация сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	

Код, наименование общих компетенций	**Критерии оценки**	**Формы и методы контроля и оценки результатов обучения**
ОК 01.Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- распознавание задач в профессиональном и/или социальном контексте; - распознавание проблем в профессиональном и/или социальном контексте; - анализ задачи и/или проблемы; - выделение составных частей задачи и/или проблемы; - определение этапов решения задачи; - выявление информации, необходимой для решения задачи и/или проблемы; - осуществление эффективного поиска информации, необходимой для решения задачи и/или проблемы;	Текущий контроль успеваемости: - опрос устный; - выполнение заданий по практике. Промежуточная аттестация: в форме дифференцированного зачета. Метод проведения промежуточной аттестации: защита отчета по практике.

	- разработка плана действия решения задачи и/или проблемы; - определение необходимых ресурсов для решения задачи и/или проблемы; - владение актуальными методами работы в профессиональной и смежных сферах; - реализация составленного плана; - оценка результата и последствий своих действий (самостоятельно или с помощью наставника).	
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- определение задач поиска информации, необходимых источников информации; - планирование процесса поиска необходимой информации; - осуществление поиска информации необходимой для выполнения задач профессиональной деятельности; - проведение анализа информации, необходимой для выполнения задач профессиональной деятельности; - осуществление интерпретации информации, необходимой для выполнения задач профессиональной деятельности; - структурирование получаемой информации; - выделение наиболее значимой в перечне информации; - оценка практической значимости результатов поиска; - оформление результатов поиска.	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- планирование собственного профессионального развития; - построение траектории собственного профессионального и личностного развития; - реализация собственного профессионального и личностного развития; - определение актуальности нормативно-правовой документации в профессиональной деятельности.	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством,	- организация работы коллектива и команды; - эффективное взаимодействие с коллегами, руководством; - эффективное взаимодействие с	

клиентами.	клиентами.	
ОК 05.Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- грамотное изложение своих мыслей на государственном языке с учетом особенностей социального и культурного контекста; - правильное оформление документов по профессиональной тематике на государственном языке.	
ОК 06.Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- понимание значимость своей специальности; - описание значимости своей специальности; - презентация структуры профессиональной деятельности по специальности; - проявление гражданско-патриотической позиции; - демонстрация осознанного поведения на основе традиционных общечеловеческих ценностей; - применение стандартов антикоррупционного поведения.	
ОК 07.Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- содействие сохранению окружающей среды; - содействие ресурсосбережению; - осуществление эффективных действий в чрезвычайных ситуациях; - соблюдение норм экологической безопасности; - определение направлений ресурсосбережения в рамках профессиональной деятельности по специальности	
ОК 08.Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- использование физкультурно-оздоровительной деятельности для укрепления здоровья, достижения жизненных и профессиональных целей; - применение рациональных приемов двигательных функций в профессиональной деятельности; - использование средств профилактики перенапряжения характерными для данной специальности	
ОК 09.Использовать информационные технологии в	- применение средств информационных технологий для решения профессиональных задач;	

профессиональной деятельности.	- использование современного программного обеспечения	
ОК 10.Пользоваться профессиональной документацией на государственном и иностранном языках.	- понимание общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые); - понимание текста на базовые профессиональные темы; - участие в диалогах на знакомые общие и профессиональные темы; - построение простых высказываний о себе и о своей профессиональной деятельности; - краткое обоснование и объяснение своих действий (текущих и планируемых); - написание простых связных сообщений на знакомые или интересующие профессиональные темы	
ОК.11. Использовать знания финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	- выявление достоинств и недостатков коммерческой идеи; - презентация идеи открытия собственного дела в профессиональной деятельности; - оформление бизнес-плана; - расчет размера выплат по процентным ставкам кредитования; - определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности; - презентация бизнес - идеи; - определение источников финансирования	

4.2. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Показатели и критерии оценивания компетенций

Показатели и критерии оценивания компетенций, описание шкал оценивания содержатся в приложении 1.

Методические материалы

Методические материалы содержатся в приложении 2.

Приложение 1

Контрольно-оценочные средства
для проведения промежуточной аттестации по практике
ПМ.02 Защита информации в автоматизированных системах
программными и программно-аппаратными средствами

1.1. Форма промежуточной аттестации: дифференцированный зачет (8 (6) семестр).

1.2. Система оценивания результатов выполнения заданий

Оценивание результатов выполнения заданий текущего контроля успеваемости, промежуточной аттестации обучающихся осуществляется на основе следующих принципов:

достоверности оценки – оценивается уровень сформированности знаний, умений, практического опыта, общих и профессиональных компетенций, продемонстрированных обучающимися в ходе выполнения задания;

адекватности оценки – оценка выполнения заданий должна проводиться в отношении тех компетенций, которые необходимы для эффективного выполнения задания;

надежности оценки – система оценивания выполнения заданий должна обладать высокой степенью устойчивости при неоднократных оценках уровня сформированности знаний, умений, практического опыта, общих и профессиональных компетенций обучающихся;

комплексности оценки – система оценивания выполнения заданий должна позволять интегративно оценивать общие и профессиональные компетенции обучающихся;

объективности оценки – оценка выполнения конкурсных заданий должна быть независимой от особенностей профессиональной ориентации или предпочтений преподавателей, осуществляющих контроль или аттестацию.

При выполнении процедур оценки заданий используются следующие основные методы:

метод экспертной оценки (привлечение к контролю и оценке специалистов предприятий и организаций);

метод расчета первичных баллов;

метод расчета сводных баллов.

Структура оценки результатов прохождения практики (отчет по практике):

- оценка отчета обучающегося о выполненной работе, содержащегося в документе «Отчет по практике»(оценивается результат выполнения заданий практики отдельно по каждой теме, определяется средний балл);
- оценка по защите практики;
- средний балл по итогам аттестации.

Используется пяти бальнаяшкала для оценивания результатов обучения:

Перевод пяти бальной шкалы учета результатов в пяти бальную оценочную шкалу:

Оценка	**Количество баллов, набранных за выполнение теоретического и практического задания, средний балл по итогам аттестации**
Оценка 5 «отлично»	4,6-5
Оценка 4 «хорошо»	3,6-4,5
Оценка 3 «удовлетворительно»	3-3,5
Оценка 2 «неудовлетворительно»	≤ 2,9

1.3. Контрольно-оценочные средства

Задание Производственной практики

Наименование разделов, тем	**Содержание задания**	**Объем часов**	**Коды компетенций, формированию которых способствует элемент программы**
Подготовительный этап производственной практики	- Согласование порядка выполнения заданий с руководителем практики от базы практики. - Прохождение инструктажа по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами	6	ОК 04-10

	внутреннего трудового распорядка предприятия/организации, являющейся базой практики. *Представить характеристику объекта практики. Использовать при составлении характеристики таблицу (Приложение А).*		
Тема 1. Анализ принципов построения систем информационной защиты производственных подразделений	**Виды работ: Анализ принципов построения систем информационной защиты производственных подразделений** **Задание 1**. Ознакомиться со структурой предприятия, определить количество структурных подразделений; разработать перечень сведений конфиденциального характера для каждого подразделения, определить уровни конфиденциальности и уровни доступа сведений конфиденциального характера *В отчете представить организационную структуру управления предприятием в виде схемы в отчете по практике, представить перечень сведений конфиденциального характера в виде таблице для каждого подразделения.*	18	ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 2.2
Тема 2. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.	**Виды работ: Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.** **Задание 2.** Проанализировать нормативно-правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами, перечислить их, дать краткую характеристику перечисленным документам. *Представить перечень нормативно-методической документации в виде таблицы в отчете по практике.*	6	ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.2
Тема 3. Анализ эффективности применяемых программно-аппаратных средств	**Виды работ: Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении** **Задание 3.** Ознакомиться со	18	ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.6

обеспечения информационной безопасности в структурном подразделении	средствами защиты информации, используемые в каждом подразделении и, в общем, на предприятии. Осуществлять мониторинг событий информационной безопасности. Участвовать в проверке технического состояния программно-аппаратных средств обеспечения информационной безопасности. *Разработать предложения по усовершенствованию и повышению эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности на предприятии.*		
Тема 4. Обеспечение учета, обработки, хранения и передачи конфиденциальной информации	**Виды работ: Обеспечение учета, обработки, хранения и передачи конфиденциальной информации** **Задание 4.** Участвовать в: - настройке параметров BIOS; - настройке ограничений на доступ к каталогам и файлам в среде ОС Windows; - настройке ограничений запуска программных продуктов в среде ОС Windows; - настройке разграничения прав доступа средствами политики безопасности ОС Windows; *В отчете описать алгоритмы настроек.* **Задание 5.** Произвести резервное копирование АС. *Описать алгоритм резервного копирования.*	18 12	ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.4
Тема 5. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы	**Виды работ: Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы** **Задание 6.** Участвовать в установке и настройке средства защиты информации от НСД. Выполнить: - настройку политики безопасности; - настройку дискреционного доступа; - настройку мандатного разграничения доступа; - блокировку внешних носителей информации. *В отчете описать алгоритмы установки и настроек.* **Задание 7.** Выполнить сравнительный	18 18	ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.1 ПК 2.5

	анализ существующих средств гарантированного уничтожения информации, осуществить обоснованный выбор средства гарантированного уничтожения информации. Произвести установку и настройку средства гарантированного уничтожения информации. *В отчете описать установку и настройку средства гарантированного уничтожения информации, описать алгоритм защищенного уничтожения информации.* **Задание 8.** Проанализировать современные программно-аппаратные средства криптографической защиты информации имеющих лицензию ФСТЭК и ФСБ России. Создать электронно-цифровую подпись. *В отчете описать алгоритм создания электронной подписи*	6	
Тема 6. Диагностика, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности	**Виды работ: Диагностика, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности** **Задание 9.** Участвовать в диагностике и устранение отказов. Участвовать в восстановление работоспособности программно – аппаратного комплекса защиты информации. *В отчете описать алгоритм устранения отказов и восстановления работоспособности программно-аппаратного средства защиты информации.*	12	ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10 ПК 2.3
Обобщение материалов и оформление отчета по практике	Обобщение материала, полученного при прохождении практики	6	ОК 01-11
Промежуточная аттестация в форме дифференцированного зачета		6	ОК 01-11 ПК 2.1- ПК 2.6
Итого		**144**	

1.3.1 Критерии оценки отчета обучающегося о выполненной работе, содержащегося в документе «Отчет по практике»

	Критерии оценки	Оценка
1	Задания практики выполнены студентом в полном объеме.	5 "отлично"

	Отчет о выполнении заданий практики содержит верное описание самостоятельно*(либо под руководством руководителя практики)* выполненных обучающимся действий в соответствии с заданиями практики. Содержит верно выполненный анализ действий (работ), данных, верные и обоснованные выводы, верно оформленные документы.	
2	Задания практики выполнены студентом в полном объеме. Отчет о выполнении заданий практики содержит верное описание самостоятельно*(либо под руководством руководителя практики)*выполненных обучающимся действий в соответствии с заданиями практики, но допущены несущественные ошибки. Анализ действий (работ), данных выполнен в полном объеме, выводы верные, при оформлении документов допущены несущественные ошибки.	4 "хорошо"
3	Задания практики выполнены студентом в полном объеме. Отчет о выполнении заданий практики содержит верное описание самостоятельно*(либо под руководством руководителя практики)*выполненных обучающимся действий в соответствии с заданиями практики, но допущены неточности и грубые ошибки, не влекущие за собой неверный результат выполненной работы в целом. Отчет содержит результаты поверхностного анализа действий (работ), данных. Отдельные выводы нельзя считать верными, целесообразными и обоснованными. При оформлении документов допущены несущественные ошибки.	3 "удовлетворительно"
4	Задания практики выполнены студентом не в полном объеме. Отчет о выполнении заданий практики содержит множественные грубые ошибки в описании самостоятельно выполненных обучающимся действий. Анализ действий (работ), данных выполнен с грубыми нарушениями, либо не выполнен. Выводы, в большей части, нельзя считать верными. Документы оформлены неверно.	2 "неудовлетворительно"

В случае, если результат выполнения заданий практики по одной из тем, содержащейся в документе «Задание на практику» будет оценен на 2 балла "неудовлетворительно", практика не может быть оценена положительно, т.к. обучающийся не освоил в полном объеме планируемые программой практики и Заданием на практику результаты освоения практики.

1.3.2. Критерии оценки защиты практики

	Критерии оценки	Оценка
1	При защите практики: студент верно комментирует работы, выполненные им на практике, оперирует в полном объеме	5 "отлично"

	фактами и владеет информацией, содержащимися в «Отчете по практике»; приводит соответствующие аргументы для доказательства правоты собственных действий (работ), выводов. Во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал. Студент правильно, полно и уверенно отвечает на поставленные вопросы.	
2	При защите практики:студент верно комментирует работы, выполненные им на практике, оперирует в достаточном объеме фактами и владеет информацией, содержащимися в «Отчете по практике"; приводит соответствующие аргументы для доказательства правоты собственных действий и выводов. Во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал. Студент правильно,с небольшими затруднениями отвечает на поставленные вопросы. Рекомендуемая оценка, содержащаяся в характеристике организации на обучающегося - "отлично", либо "хорошо".	4 "хорошо"
3	При защите практики: студент отчасти верно комментирует работы, выполненные им на практике, демонстрирует затруднение оперируя фактами и информацией, содержащейся в «Отчете по практике"; приводит не всегда верные аргументы для доказательства правоты собственных действий. Во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал. Студент не дает полных, аргументированных ответов на заданные вопросы, но большинство ответов можно считать верными. Рекомендуемая оценка, содержащаяся в характеристике организации на обучающегося - "удовлетворительно".	3 "удовлетворительно"
4	При защите практики: студент затрудняется пояснить действия, которые он выполнял на практике в соответствии с заданиями, привести аргументы, доказывающие правоту собственных действий, объяснить выводы. На защите отсутствуют наглядные пособия или раздаточный материал. Рекомендуемая оценка, содержащаяся в характеристике организации на обучающегося - "удовлетворительно", либо "неудовлетворительно".	2 "неудовлетворительно"

Перевод десятичной дроби, полученной в результате определения среднего балла по итогам аттестации, в пяти бальную оценочную шкалу:

Оценка	**Количество баллов, набранных за выполнение задания учебной практики, средний балл по итогам аттестации**
Оценка 5 «отлично»	**4,6-5**

Оценка 4 «хорошо»	**3,6-4,5**
Оценка 3 «удовлетворительно»	**3-3,5**
Оценка 2 «неудовлетворительно»	**≤ 2,9**

1.4. Материально-техническое обеспечение для проведения промежуточной аттестации

Аттестация проводится в лаборатории программных и программно-аппаратных средств защиты информации.

1.5. Учебно-методическое и информационное обеспечение для проведения промежуточной аттестации

Нормативно-правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». - Режим доступа: http://www.consultant.ru/
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». - Режим доступа: http://www.consultant.ru/
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». - Режим доступа: http://www.consultant.ru/
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». - Режим доступа: http://www.consultant.ru/
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». - Режим доступа: http://www.consultant.ru/
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». - Режим доступа: http://www.consultant.ru/
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». - Режим доступа: http://www.consultant.ru/
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». - Режим доступа: http://www.consultant.ru/
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608. - Режим доступа: http://www.consultant.ru/
10. Приказ ФСТЭК России от 17.07.2017 N 134 (ред. от 17.12.2019) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" (Зарегистрировано в Минюсте России 09.08.2017 N 47722) - Режим доступа: http://www.consultant.ru/
11. Приказ ФСТЭК России от 12.07.2012 N 84 (ред. от 20.05.2015) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной

информации" (Зарегистрировано в Минюсте России 20.08.2012 N 25220) - Режим доступа: http://www.consultant.ru/

12. Приказ ФАПСИ 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». - Режим доступа: http://www.consultant.ru/

13. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». - Режим доступа: http://www.consultant.ru/

14. 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. – Режим доступа: http://docs.cntd.ru/

15. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – Режим доступа: http://docs.cntd.ru/

16. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Режим доступа: http://docs.cntd.ru/

17. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – Режим доступа: http://docs.cntd.ru/

18. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Практические правила управления информационной безопасностью. – Режим доступа: http://docs.cntd.ru/

19. 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. – Режим доступа: http://docs.cntd.ru/

20. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Режим доступа: http://docs.cntd.ru/

21. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Режим доступа: http://docs.cntd.ru/

22. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Режим доступа: http://docs.cntd.ru/

23. ГОСТ 34.311-95 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (аутентичен ГОСТ Р 34.11-94). – Режим доступа: http://docs.cntd.ru/

24. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

25. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Режим доступа: http://docs.cntd.ru/

26. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

27. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Режим доступа: http://docs.cntd.ru/

28. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

29. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/

30. 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. – Режим доступа: http://docs.cntd.ru/

31. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

32. 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. – Режим доступа: http://docs.cntd.ru/

33. 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. – Режим доступа: http://docs.cntd.ru/

34. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

35. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

Основные учебные издания

36. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлинский; под ред. В.Н. Пржегорлинского. - 1-е изд. - М. : Издательский центр «Академия», 2020. – 288 с. В пер. ISBN 978-5-4468-8717-0

37. 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. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

38. 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. —

(Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

39. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности / учеб. пособие для студ. учреждений сред. проф. образования / Е.Б. Белов, В.Н. Пржегорлинский. - 2-е изд., испр. и доп. - М. : Издательский центр «Академия», 2020. – 336 с. В пер. ISBN 978-5-4468-8456-8

40. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

41. Костров Б.В. Сети и системы передачи информации : учебник/ Б.В. Костров, В.Н. Ручкин : (2-е изд.) (в электронном формате) 2019. https://academia-library.ru

42. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина; под ред. В.Н. Пржегорлинского.- 1-е изд. - М. : Издательский центр «Академия», 2019. – 272 с. В пер. ISBN 978-5-4468-8718-7

43. Бубнов А.А. Основы информационной безопасности : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, О.А. Савинкин. - 3-е изд., стер. - М. : Издательский центр «Академия», 2020. – 256 с. В пер. ISBN 978-5-4468-8682-1

Дополнительные учебные издания

44. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Режим доступа: http://www.consultant.ru/

46. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Режим доступа: http://www.consultant.ru/

47. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/

48. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/

49. 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. – Режим доступа: http://docs.cntd.ru/

50. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - Режим доступа: http://www.consultant.ru/

51. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

52. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Режим доступа: http://www.consultant.ru/

53. 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. - Режим доступа: http://www.consultant.ru/

Интернет-ресурсы

54. Сайт журнала Информационная безопасность - Режим доступа: http://www.itsec.ru

55. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/

56. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/

57. Федеральный портал. Российское образование. - Режим доступа:http://www.edu.ru

Методические указания по выполнению заданий практики

58. Методические указания по выполнению заданий практики.