МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»
(СГТУ имени Гагарина Ю.А.)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ

УТВЕРЖДАЮ
Директор ППК СГТУ имени Гагарина Ю.А.
_____ М.Ю. Захарченко
_____ 2019 г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ ПО СПЕЦИАЛЬНОСТИ 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

г. Саратов 2019

Рабочая программа Производственной (преддипломной) 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.

Разработчики:

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

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

Рецензенты:

Внутренний: Ястребова М.А.– преподаватель высшей квалификационной категории Профессионально-педагогического колледжа СГТУ имени Гагарина Ю.А.

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

СОДЕРЖАНИЕ

Стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

1.1. Область применения рабочей программы

Рабочая программа Производственной (преддипломной) практики является частью программы подготовки специалистов среднего звена (далее - ППССЗ) в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Производственная (преддипломная) практика проводится после освоения обучающимися профессиональных модулей: ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении», ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами», ПМ.03 «Защита информации техническими средствами».

1.2. Место практики в структуре ППССЗ.

Производственная (преддипломная) практика входит в Профессиональный цикл.

1.3. Цели и требования к результатам освоения практики

Производственная (преддипломная) практика направлена на углубление практического опыта обучающегося, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы в организациях различных организационно-правовых форм.

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.

1.3.2. Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
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.
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.3.3. В результате освоения программы практики обучающийся должен:

Углубить практический опыт в:

- эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;
- администрировании автоматизированных систем в защищенном исполнении;
- установке компонентов систем защиты информации автоматизированных информационных систем;
- 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;
- выявлении технических каналов утечки информации;
- применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;
- проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
- проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

1.4. Количество часов на освоение программы практики:

Всего: 144 часа.

2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

2.1. Тематический план практики

Код (ПК, ОК)	**Количество часов практики**	**Наименования разделов практики**	**Количество часов по разделам**
1	2	3	4
ПК 1.1-1.4 ПК 2.1-2.6 ПК 3.1-3.5 ОК 01-10	144	Инструктаж	**6**
		ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами.	**126**
		Обобщение материалов, оформление дневника и отчета по практике.	**6**
		Промежуточная аттестация в форме дифференцированного зачета	**6**

2.2. Содержание практики

Наименование разделов, тем практики	Видыработ	Объем часов	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4	5
Инструктаж	- Согласовать порядок выполнения заданий с руководителем практики от колледжа. - Пройти инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности	6	1	ОК 01-10
Тема 1. Сети и системы передачи информации, операционные системы, базы данных	1. Администрирование программных компонентов автоматизированной (информационной) системы. 2. Администрирование сетевых ресурсов.	12	3	ОК 01-10 ПК 1.1 ПК 1.2
Тема 2. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	3.Обеспечение бесперебойной работы автоматизированных (информационных) систем.	6	3	ОК 01-10 ПК 1.3
Тема 3. Эксплуатация компьютерных сетей	4. Обеспечение сетевой безопасности.	12	3	ОК 01-10 ПК 1.4
Тема 4. Программные и программно-аппаратные средства защиты информации	5.Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами. 6.Мониторинг эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности. 7.Обеспечение защиты информации в автоматизированных (информационных) системах отдельными программными, программно-аппаратными средствами.	72	3	ОК 01-10 ПК 2.1 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6
Тема 5. Криптографические средства защиты информации	8. Использование типовых криптографических средств и методов защиты информации.	12	3	ОК01-10 ПК 2.2
Тема 6. Техническая защита информации	9.Участие в обслуживании и эксплуатации технических средств защиты информации.	6	3	ОК 01-10 ПК 3.1 ПК 3.2

				ПК 3.3 ПК 3.4
Тема 7. Инженерно-технические средства физической защиты объектов информатизации	10.Участие в обслуживании и эксплуатации средств инженерно-технической защиты.	6	3	ОК 01-10 ПК 3.5
Обобщение материалов, оформление дневника и отчета по практике.		6	3	ОК 01-10 ПК 1.1-1.4 ПК 2.1-2.6 ПК 3.1-3.5
Промежуточная аттестация в форме дифференцированного зачета		6	3	ОК 01-10 ПК 1.1-1.4 ПК 2.1-2.6 ПК 3.1-3.5
Всего:		***144***		

3. УСЛОВИЯ РЕАЛИЗАЦИИПРОГРАММЫ 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.
30. Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/
31. 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/
32. 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/
33. 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/
34. 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/

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

36. 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

1. Батаев А.В. Операционные системы и среды: учебник для студ. учреждений сред.проф. образования /А.В. Батаев, Н.Ю. Налютин, С.В. Синицын.- 2-е изд., стер.- Москва: Издательский центр "Академия", 2018.- 272с. ISBN 978-5-4468-6801-8

2. 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

3. 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

4. Компьютерные сети: учебник для студ. учреждений сред.проф. образования /В.В. Баринов, И.В. Баринов, А.В. Пролетарский, А.Н. Пылькин.- Москва: Издательский центр "Академия", 2018.- 192с. ISBN 978-5-4468-7192-6

5. 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

6. 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

7. 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.

8. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД "ФОРУМ" : ИНФРА-М, 2021. - 416 с. - (Среднее профессиональное образование). ISBN 978-5-8199-0754-2

Дополнительные учебные издания

1. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

2. Гостев, И. М. Операционные системы: учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

3. 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

4. Новикова Е.Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: учебник для СПО /Е.Л. Новикова.- Москва: Издательский центр "Академия", 2018.- 192с. ISBN 978-5-4468-5777-7

5. 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

6. 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

7. 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/

8. 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/

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

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

11. 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/

12. 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/

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

14. 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/

15. 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/

16. 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

17. 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/

18. 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/

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

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

21. 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/

22. 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/

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

24. 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/

25. 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

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей - Режим доступа: https://ichip.ru/

2. Журналы Защита информации. Инсайд: Информационно-методический журнал - Режим доступа: http://www.inside-zi.ru/

3. Информационная безопасность регионов: Научно-практический журнал- Режим доступа: https://www.elibrary.ru/title_about.asp?id=28126

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

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

6. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) - Режим доступа: https://fstec.ru/

7. Информационно-справочная система по документам в области технической защиты информации - Режим доступа: https://fstec.ru/

8. Информационный портал по безопасности - Режим доступа: www.SecurityLab.ru.

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

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

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

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

13. Российский биометрический портал - Режим доступа: http://www.biometrics.ru/

14. Сайт Научной электронной библиотеки - Режим доступа: https://www.elibrary.ru/

Методические указания по выполнению заданий практики

1. Методические указания по выполнению заданий практики.

3.3. Общие требования к организации образовательного процесса

Образовательная деятельность при освоении профессиональных модулей организуется в форме практической подготовки путем проведении всех видов практик, предусматривающих непосредственное выполнение обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Производственная(преддипломная) практика проводится после освоения обучающимися всех разделов, входящих в профессиональные модули и реализуется концентрированно. Производственная (преддипломная) практика реализуется в профильных организациях, в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки.

3.4. Кадровое обеспечение образовательного процесса

Для реализации программы Производственной (преддипломной) 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 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	установка компонентов систем защиты информации автоматизированных информационных систем; обеспечение работоспособности, обнаружение и устранение неисправностей, осуществление комплектования, конфигурирования, настройки автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;	**Текущий контроль:** собеседование по результатам выполненной работы, наблюдение за процессом выполнения заданий. выполнение письменной работы «Отчет по практике» **Промежуточная аттестация**: отчет по практике.
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	администрирование автоматизированных систем в защищенном исполнении; обеспечение работоспособности, обнаружение и устранение неисправностей, осуществление комплектования, конфигурирования, настройки автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; установка, адаптация и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; конфигурация, монтаж, осуществление диагностики компьютерных сетей; устранение неисправностей компьютерных сетей; работа с сетевыми протоколами разных уровней;	
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями	эксплуатация компонентов систем защиты информации автоматизированных систем; настройка и устранение неисправностей программно-аппаратных средств защиты	

эксплуатационной документации	информации в компьютерных сетях по заданным правилам;	
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении	диагностика, устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем; обеспечение работоспособности, обнаружение и устранение неисправностей, осуществление комплектования, конфигурирования, настройки автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;	
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	
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	применение, техническое обслуживание, диагностика, устранение отказов, восстановление работоспособности, установка, монтаж и настройка инженерно-технических средств физической защиты и технических 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 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;	
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	выявление технических каналов утечки информации; применение средств охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	

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; 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).	Текущий контроль успеваемости: - опрос устный; - выполнение заданий по практике. Промежуточная аттестация: в форме дифференцированного зачета. Метод проведения промежуточной аттестации: защита отчета по практике.
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, клиентами.	организация работы коллектива и команды; эффективное взаимодействие с коллегами, руководством; эффективное взаимодействие с 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	применение средств	

информационные технологии в профессиональной деятельности.	информационных технологий для решения профессиональных задач; 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	

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

1.1. Форма промежуточной аттестации: дифференцированный зачет

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 пятибалльная шкала для оценивания результатов обучения:

Перевод пятибалльной шкалы учета результатов в пятибалльную 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 (преддипломной) практики

Наименование разделов, тем	Содержание задания	Объем часов	Коды компетенций, формированию которых способствует элемент программы
Подготовительный этап производственной (преддипломной) 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 внутреннего трудового распорядка предприятия/организации, являющейся базой практики. *Представить характеристику объекта практики в отчете по практике. Использовать при составлении характеристики таблицу* (Приложение Д)	6	ОК 01-10
ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»			
Тема 1. Сети и системы передачи информации, операционные системы, базы данных	**Вид работ: администрирование сетевых ресурсов.** **Задание 1.** Определить сетевые ресурсы (аппаратные, программные, информационные) предприятия/организации. Определить категории (группы) пользователей на предприятия/организации и их права доступа к сетевым ресурсам. Выполнить настройки ограничения прав пользователей, ограничения использования средств хранения информации (USB) на рабочих местах. *В отчете предоставить:* - *перечень сетевых ресурсов в виде таблицы;* - *распределение прав доступа к сетевым*	6	ОК 01-10 ПК 1.1 ПК 1.2

	ресурсам по категориям (группам) пользователей в виде таблицы; *- описание настроек ограничения прав пользователей, ограничения использования средств хранения информации (USB) на рабочих местах.* **Вид работ: администрирование программных компонентов автоматизированной (информационной) системы.** **Задание 2.** Настроить средства антивирусной защиты для корректной работы программного обеспечения. *В отчете описать настройку средств антивирусной защиты.* **Задание 3.** Выполнить проверку работоспособности системы защиты информации автоматизированной системы. *В отчете описать:* *- проверку доступности портов;* *- проверку ограничения прав пользователей;* *- проверку запрета использования переносных носителей информации;* *- проверку работоспособности антивирусной защиты.*	2 4	
Тема 2. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**Вид работ: обеспечение бесперебойной работы автоматизированных (информационных) систем.** **Задание 4.** Настроить встроенные средства защиты информации программного обеспечения. Осуществлять проверку функционирования встроенных средств защиты информации программного обеспечения. *В отчете описать:* *- настройку брендмауера;* *- настройку фаервола ОС;* *- настройку средств аутентификации пользователей;* *- настройку шифрования информации встроенными средствами ОС (утилиты шифрования данных ОС).*	6	ОК 01-10 ПК 1.3
Тема 3. Эксплуатация компьютерных сетей	**Вид работ: обеспечение сетевой безопасности.** **Задание 5.** Ознакомиться с архитектурой компьютерной сети предприятия/организации. Определить средства выхода в интернет, используемые технологии и оборудование. Проанализировать угрозы безопасности информации, методы и средства защиты информации, используемые на предприятии/организации. Разработать комплекс мероприятий по защите информации в компьютерной сети. *В отчете представить:* *- план помещений предприятия/организации*	12	ОК 01-10 ПК 1.4

	со структурной схемой компьютерной сети; *- перечень угроз безопасности информации;* *- модель комплексной защиты информации в компьютерной сети с описанием рекомендаций.*		
ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»			
Тема 4. Программные и программно-аппаратные средства защиты информации	**Вид работ: применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами.** **Задание 6.** Проанализировать нормативно-правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами, перечислить их, дать краткую характеристику перечисленным документам. *В отчете представить перечень нормативно-методической документации в виде таблицы.* **Вид работ: анализ принципов построения системы информационной защиты.** **Задание 7.** Разработать перечень сведений конфиденциального характера для каждого подразделения предприятии/организации, определить уровни конфиденциальности и уровни доступа сведений конфиденциального характера. *В отчете представить перечень сведений конфиденциального характера в виде таблице для каждого подразделения.* **Задание 8.** Проанализировать способы (методы) обеспечения учета, обработки, хранения и передачи информации ограниченного доступа на предприятии/организации. Проанализировать информационную систему на предмет имеющихся/возможных уязвимостей, выявить причины обнаруженных уязвимостей, определить их возможные последствия. *В отчете представить таблицу, в которой необходимо отразить:* *- способ/метод учета/обработки/хранения/передачи информации ограниченного доступа;* *- имеющиеся/возможные уязвимости представленного способ/метод;* *- причины обнаруженных уязвимостей;* *- возможные последствия обнаруженных уязвимостей.*	6 6 6	ОК 01-10 ПК 2.1 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6

	Вид работ: мониторинг эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности. **Задание 9.** Провести выбор системы мониторинга событий информационной безопасности. Проанализировать сообщения о событиях безопасности, поступающих от средств защиты, операционных систем, прикладного программного обеспечения и телекоммуникационное обеспечение. Произвести проверку технического состояния программно-аппаратных средств обеспечения информационной безопасности. *В отчете:* *- представить из журнала событий выписку зарегистрированных сведений об осуществлении логического доступа к информационному ресурсу;* *- сделать вывод об эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности;* *- сделать вывод о результатах тестирования технического состояния программно-аппаратных средств обеспечения информационной безопасности.* **Вид работ: обеспечение защиты информации в автоматизированных (информационных) системах отдельными программными, программно-аппаратными средствами.** **Задание 10.** Разработать требования к проектируемой системе защиты. *В отчете предоставить техническое задание на проектируемую систему.* **Задание 11.** Осуществить выбор максимально эффективного способа защиты информации в автоматизированной (информационной). *В отчете предоставить описание выбранного способа защиты информации.* **Задание 12.** Выполнить сравнительный анализ существующих средств гарантированного уничтожения информации, осуществить обоснованный выбор средства гарантированного уничтожения информации. *В отчете предоставить сравнительную таблицу средств гарантированного уничтожения информации.* **Задание 13.** Смоделировать проектируемую систему защиты информации. *В отчете предоставить графическую*	12 6 6 12	

	модель системы защиты (при построении опираться на типовые модели - Приложение Е). **Задание 14.** Выполнить установку и настройку программно-аппаратного средства защиты информации. Протестировать установленное программно-аппаратное средство защиты информации. *В отчете предоставить:* *- описание установки и настройки программно-аппаратного средства защиты информации;* *- описание процесса тестирования программно-аппаратного средства защиты информации.*	12	
Тема 5. Криптографические средства защиты информации	**Вид работ: использование типовых криптографических средств и методов защиты информации.** **Задание 15.** Проанализировать современные криптографические средства и методы защиты информации. Выполнить установку и настройку выбранного криптографического средства или метода (в том числе электронной подписи). Протестировать установленное криптографическое средство или метод. *В отчете предоставить:* *- сравнительную таблицу криптографических средств и методов;* *- описание установки и настройки криптографического средства или метода (в том числе электронной подписи);* *- описание процесса тестирования криптографического средства или метода.*	12	ОК 01-10 ПК 2.2
ПМ.03 «Защита информации техническими средствами»			
Тема 6. Техническая защита информации	**Вид работ: участие в обслуживании и эксплуатации технических средств защиты информации.** **Задание 16.** Проанализировать методы и средства технической защиты информации, применяемые на предприятии/организации. Разработать рекомендации по более эффективной работе технических средств защиты информации. *В отчете предоставить рекомендации в виде таблицы, в которой отразить:* *- наименование защищаемой информации;* *- вид угрозы;* *- ИТСЗ применяемые на предприятии;* *- рекомендации.*	6	ОК 01-10 ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4
Тема 7. Инженерно-технические средства **физической защиты** объектов информатизации	**Вид работ: участие в обслуживании и эксплуатации средств инженерно-технической защиты.** **Задание 17.** Проанализировать методы и средства инженерно-технической защиты информации, применяемые на	6	ОК 01-10 ПК 3.5

	предприятии/организации. Разработать рекомендации по более эффективной работе средств инженерно-технической защиты информации. *В отчете предоставить рекомендации в виде таблицы, в которой отразить:* *- контролируемая зона;* *- ИТСЗИ используемые на предприятии/организации;* *- результаты проверки технического состояния ИТСЗИ;* *- рекомендации.*		
Обобщение материалов и оформление отчета по практике.	Обобщение материала, полученного при прохождении практики	6	ОК 01-10 ПК 1.1-1.4 ПК 2.1-2.6 ПК 3.1-3.5
Промежуточная аттестация в форме дифференцированного зачета		6	
Всего		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. 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.	5 «отлично»
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.	3 «удовлетворительно»

	Отчет содержит результаты поверхностного анализа действий (работ), данных. Отдельные выводы нельзя считать верными, целесообразными и обоснованными. При оформлении документов допущены несущественные ошибки.	
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 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.	5 «отлично»
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 сетей и систем передачи информации, лаборатории программных и программно-аппаратных средств защиты информации, лаборатории технических 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.

30. Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/

31. 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/

32. 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/

33. 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/

34. 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/

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

36. 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

1. Батаев А.В. Операционные системы и среды: учебник для студ. учреждений сред.проф. образования /А.В. Батаев, Н.Ю. Налютин, С.В. Синицын.- 2-е изд., стер.- Москва: Издательский центр "Академия", 2018.- 272с. ISBN 978-5-4468-6801-8

2. 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

3. 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

4. Компьютерные сети: учебник для студ. учреждений сред.проф. образования /В.В. Баринов, И.В. Баринов, А.В. Пролетарский, А.Н. Пылькин.- Москва: Издательский центр "Академия", 2018.- 192с. ISBN 978-5-4468-7192-6

5. 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

6. 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

7. 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.
8. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД "ФОРУМ" : ИНФРА-М, 2021. - 416 с. - (Среднее профессиональное образование). ISBN 978-5-8199-0754-2

Дополнительные учебные издания

1. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru
2. Гостев, И. М. Операционные системы: учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru
3. 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
4. Новикова Е.Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: учебник для СПО /Е.Л. Новикова.- Москва: Издательский центр "Академия", 2018.- 192с. ISBN 978-5-4468-5777-7
5. 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
6. 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
7. 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/
8. 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/
9. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/
10. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/
11. 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/

12. 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/

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

14. 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/

15. 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/

16. 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

17. 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/

18. 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/

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

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

21. 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/

22. 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/

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

24. 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/

25. 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

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей - Режим доступа: https://ichip.ru/
2. Журналы Защита информации. Инсайд: Информационно-методический журнал - Режим доступа: http://www.inside-zi.ru/
3. Информационная безопасность регионов: Научно-практический журнал-Режим доступа: https://www.elibrary.ru/title_about.asp?id=28126
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. - Режим доступа: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. - Режим доступа: http://bit.mephi.ru/
6. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) - Режим доступа: https://fstec.ru/
7. Информационно-справочная система по документам в области технической защиты информации - Режим доступа: https://fstec.ru/
8. Информационный портал по безопасности - Режим доступа: www.SecurityLab.ru.
9. Сайт журнала Информационная безопасность - Режим доступа: http://www.itsec.ru
10. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/
11. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/
12. Федеральный портал. Российское образование. - Режим доступа:http://www.edu.ru
13. Российский биометрический портал - Режим доступа: http://www.biometrics.ru/
14. Сайт Научной электронной библиотеки - Режим доступа: https://www.elibrary.ru/

Методические указания по выполнению заданий практики

1. Методические указания по выполнению заданий практики.