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» _____ 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
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 учебной дисциплины 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

Разработчик: Орлова Н. Л. - преподаватель ППК 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

1.	**ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**	**4**
2.	**СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**	**7**
3.	**УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**	**9**
4.	**КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**	**10**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП. 01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения рабочей программы

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

1.2. Место учебной дисциплины в структуре ППССЗ:

Дисциплина входит в профессиональный учебный цикл, в состав общепрофессиональных дисциплин.

1.3 Цели и требования к результатам освоения учебной дисциплины

Изучение дисциплины направлено на формирование общих и профессиональных компетенций, включающих в себя способность:

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

В результате освоения учебной дисциплины обучающийся должен **уметь:**

– классифицировать защищаемую информацию по видам тайны и степеням секретности;

– классифицировать основные угрозы безопасности информации;

В результате освоения учебной дисциплины обучающийся должен **знать:**

– сущность и понятие информационной безопасности, характеристику ее составляющих;

– место информационной безопасности в системе национальной безопасности страны;

– виды, источники и носители защищаемой информации;

– источники угроз безопасности информации и меры по их предотвращению;

– факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

– жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

– современные средства и способы обеспечения информационной безопасности;

– основные методики анализа угроз и рисков информационной безопасности.

1.4.Количество часов на освоение программы учебной дисциплины:

Максимальной учебной нагрузки обучающегося: 66 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 48 часов;

самостоятельной работы обучающегося 6 часов;

промежуточной аттестации 12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего по программе дисциплины)	66
Промежуточная аттестация	12
Обязательная аудиторная учебная нагрузка (всего)	48
в том числе:	
лекции, уроки	30
практические занятия	18
Самостоятельная работа обучающегося (всего)	6
Промежуточная аттестация в форме экзамена	

2.2. Тематический план и содержание учебной дисциплины ОП.01 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект) (если предусмотрены), иные виды учебной работы в соответствии с учебным планом	Объем часов	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4	5
Раздел 1. Теоретические основы информационной безопасности		**30**		
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	**4**		ОК 3, ОК 6, ОК 9, ПК.2.4
	Понятие информации и информационной безопасности. Составляющие и аспекты информационной безопасности.	2	1	
	Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	2		
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	**16**		
	Цели и задачи защиты информации. Основные понятия в области защиты информации.	2		
	Обзор защищаемых объектов и систем. Сущность функционирования системы защиты информации.	2		
	Понятие Политики безопасности.	2		
	Практическое занятие №1. Определение объектов защиты на типовом объекте информатизации.	4	2	
	Практическое занятие №2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	4		
	Практическое занятие №3. Формирование структуры политики безопасности на примере типового предприятия.	2		
Тема 1.3. Угрозы	**Содержание учебного материала**	**10**		

безопасности защищаемой информации.	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.	2	1	
	Каналы и методы несанкционированного доступа к информации	2		
	Уязвимости. Методы оценки уязвимости информации	2		
	Практическое занятие №4.Определение угроз объекта информатизации и их классификация	4	2	
Раздел 2. Методология защиты информации		**24**		
Тема 2.1. Методологические подходы к защите информации	**Содержание учебного материала**	**6**		ОК 3, ОК 6, ОК 9, ОК 10 ПК 2.4
	Анализ существующих методик определения требований к защите информации.	2	1	
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	2		
	Виды мер и основные принципы защиты информации.	2		
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание учебного материала**	**10**		
	Организационная структура системы защиты информации	2		
	Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации.	2		
	Самостоятельная работа обучающихся №1 Работа над проектом «Информационная безопасность РФ»	6	3	
Тема 2.3. Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала**	**8**		
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	2	1	
	Программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации	2		
	Практическое занятие №5.Выбор мер защиты информации для автоматизированного рабочего места	4	2	
Промежуточная аттестация – экзамен		**12**		
Итого по дисциплине:		**66**		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует кабинета информатики для проведения занятий лекционного типа, практических занятий, в том числе групповых, индивидуальных, письменных, устных консультаций, текущего контроля и промежуточной аттестации.

Оборудование:

- рабочее место преподавателя;
- специализированная мебель (столы, стулья по количеству обучающихся);
- доска ученическая.

Технические средства обучения:

- компьютер (ноутбук);
- мультимедийный проектор, экран.

Учебно-наглядные пособия: плакаты, учебно-наглядные пособия, обеспечивающие тематические иллюстрации по рабочей программе дисциплины, в том числе, видео-аудио материалы, компьютерные презентации.

Компьютер имеет доступ к электронно-библиотечным системам, выход в глобальную сеть Интернет, оснащен лицензионным программным обеспечением.

3.2. Учебно-методическое и информационное обеспечение реализации учебной дисциплины

Основные учебные издания

1. 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

2. 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/

3. Информационная безопасность : учебник / Мельников В.П., под ред., Куприянов А.И. — Москва : КноРус, 2021. — 267 с. — ISBN 978-5-406-08259-1. — URL: https://book.ru

Дополнительные учебные издания

4. 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

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. 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

Интернет-ресурсы

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

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

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

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

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

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

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

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

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

16. Федеральный портал. Российское образование. - Режим доступа: http://www.edu.ru
17. Российский биометрический портал - Режим доступа: http://www.biometrics.ru/
18. Сайт Научной электронной библиотеки - Режим доступа: https://www.elibrary.ru/

Методические рекомендации для обучающихся по освоению дисциплины

19. Методические указания для обучающихся по выполнению практических работ.
20. Методические указания для обучающихся по выполнению заданий самостоятельной работы.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Формы и методы контроля и оценки результатов обучения

Результаты обучения	Формы и методы контроля и оценки результатов обучения
Общие компетенции: ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. ОК 09. Использовать информационные технологии в профессиональной деятельности. ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках. **Профессиональные компетенции:** ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. **Уметь:** - классифицировать защищаемую информацию по видам тайны и степеням секретности; - классифицировать основные угрозы безопасности информации; **Знать:** - сущность и понятие информационной безопасности, характеристику ее составляющих; - место информационной безопасности в системе национальной безопасности страны; - виды, источники и носители защищаемой информации; - источники угроз безопасности информации и меры по их предотвращению; - факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; - жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; - современные средства и способы обеспечения информационной безопасности; - основные методики анализа угроз и рисков информационной безопасности.	Текущий контроль: - опрос устный (фронтальный); - тестирование; - выполнение письменной работы; - выполнение практической работы; Оценка результатов выполнения самостоятельной работы Промежуточная аттестация в форме экзамена. Метод проведения промежуточной аттестации 3 семестра: выполнение экзаменационного задания

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

Показатели и критерии оценивания компетенций

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

Контрольные и тестовые задания

Контрольные задания содержатся в приложении 1.

Методические материалы

Методические материалы, определяющие процедуры оценивания знаний, умений, характеризующих формирование компетенций, содержатся в приложении 1.

Приложение 1

Контрольно-оценочные средства

для проведения промежуточной аттестации по дисциплине
ОП.01 Основы информационной безопасности

1.1. Форма промежуточной аттестации: Экзамен (3 семестр).

1.2. Система оценивания результатов выполнения заданий

Оценивание результатов выполнения заданий промежуточной аттестации 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 расчета первичных баллов;

– метод расчета сводных баллов.

Результаты выполнения заданий оцениваются в соответствии с разработанными критериями оценки.

Используется пяти бальная шкала 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

1.3.1 Задание:

1.Ответить на вопросы теста.

2. Выполнить практическое задание.

Примерные вопросы для тестирования

1. **Преднамеренная угроза безопасности информации**
a) Кража
b) Наводнение
c) повреждение кабеля, по которому идет передача, в связи с погодными условиями
d) ошибка разработчика
2. **Виды информации по способу восприятия информации человеком**
a) текстовая, числовая, графическая, табличная
b) научная, социальная, политическая, экономическая, религиозная
c) обыденная, производственная, техническая, управленческая
d) визуальная, звуковая, тактильная, обонятельная, вкусовая
e) математическая, биологическая, медицинская, психологическая
3. **Информационный процесс обеспечивается…**
a) информационными системами и средствами передачи данных
b) программным обеспечением
c) аппаратным (техническим) обеспечением
d) коммуникационными каналами
4. **Атака – это попытка реализации _____**
5. **Какой из терминов определяется как состояние защищённости национальных интересов в информационной сфере и совокупностью сбалансированных интересов личности, общества и государства:**
a) Конфиденциальность;
b) Аутентичность;
c) Информационная безопасность;
d) Ограниченность доступа.
6. **Общий процесс анализа и оценивания риска:**
a) Принятие риска
b) Предотвращение риска
c) Оценка риска
d) Оценивание риска
7. **Какой из терминов определяется как потенциальная причина инцидента, способная нанести ущерб системе или организации:**
a) Угроза;
b) Опасность;
c) Нападение.
8. **Какой из терминов определяется как неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации:**
a) Утечка
b) Уязвимость
c) Разглашение
9. **Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется**
a) системой угроз;
b) системой защиты;
c) системой безопасности
d) системой уничтожения

10. **Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется**

a) угрозой;
b) опасностью;
c) намерением;
d) предостережением.

11. **Что такое криптография?**

a) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
b) область доступной информации
c) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом

12. **Конфиденциальность – это..**

a) защита от несанкционированного доступа к информации
b) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
c) описание процедур

13. Сбой – **это такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент**

14. **Побочное влияние – это…**

a) негативное воздействие на систему в целом или отдельные элементы
b) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
c) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

15. **Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают:**

a) средства выявления злоумышленной активности;
b) средства обеспечения отказоустойчивости;
c) средства контроля эффективности защиты информации

16. **Документы, содержащие государственную тайну не снабжаются грифом**

a) "секретно"
b) "совершенно секретно"
c) “строго конфиденциально”
d) "особой важности"

17. Отказ – **это нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций**

18. **Самыми опасными источниками внутренних угроз являются:**

a) некомпетентные руководители;
b) обиженные сотрудники;
c) любопытные администраторы.

19. **Контроль целостности может использоваться для:**

a) предупреждения нарушений И Б;
b) обнаружения нарушений;
c) локализации последствий нарушений.

20. **Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и при успешности, предоставление ему определенных полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом**

a) Авториза́ция
b) Идентификация
c) Аутентификация
d) Обезличивание
e) Деперсонализация

21. **Криптография необходима для реализации следующих сервисов безопасности:**
a) идентификация;
b) экранирование;
c) аутентификация.

22. **Формой правовой защиты литературных, художественных и научных произведений является (...) право**
a) литературное
b) художественное
c) авторское
d) патентное

23. Вирус – **это код обладающий способностью к распространению путем внедрения в другие программы**

24. **Дублирование сообщений является угрозой:**
a) доступности;
b) конфиденциальности**;**
c) целостности.

25. **Протоколирование и аудит могут использоваться для:**
a) предупреждения нарушений И Б;
b) обнаружения нарушений;
c) восстановления режима И Б.

Примерные практические задания:

1. Определите в каких формах представлена информация на вашей домашней ЭВМ. Опишите, как обеспечивается информационная безопасность вашей ПЭВМ и отвечает ли современным требованиям развития систем безопасности.
2. Зашифруйте текст “Информационные системы и технологии” по шифру Цезаря, где K=2.
3. Дана ситуация – разговор в помещении или на улице. Укажите виды каналов утечки информации, методы и средства получения и защиты информации в данном случае.
4. Постройте диаграмму причин компьютерных преступлений.
5. Угроза – утечка или кража личных данных. Ваши действия, чтобы обезопасить себя от подобных воздействий.

1.3.2. Критерии оценки

Максимальное количество баллов за выполнение задания «Тестирование» – 2 балла.

Оценка за задание «Тестирование» определяется простым суммированием баллов за правильные ответы на вопросы. Один верный ответ равен 0,08 балла.

Ответ считается правильным, если:
- при ответе на вопрос закрытой формы с выбором ответа выбран правильный ответ;
- при ответе на вопрос открытой формы дан правильный ответ;

	Критерии оценки результатов выполнения практического задания	Баллы за критерии оценки
	Выполнение практического задания	**Максимальный балл – 3,0 балла**
1	Соответствует условиям задачи	0,3
2	Присутствует логика решения	0,3
3	Оформление решения задачи соответствует требованиям	0,3
4	При выполнении соблюдена последовательность действий	0,3
5	Использованы термины и обозначения дисциплины	0,3
6	Правильно выбраны отдельные элементы задания	0,3
	Устное собеседование по заданию	
7	Анализ ситуации проведен верно	0,3
8	Обоснование решения ведется грамотно	0,3
9	Приводятся аргументированные примеры	0,3
10	Приведены выводы и/или ссылки на соответствующие документы	0,3

1.4. Материально-техническое обеспечение для проведения промежуточной аттестации

Аттестация проводится в кабинете информатики.

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

Основные учебные издания

1. 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

2. 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/

3. Информационная безопасность : учебник / Мельников В.П., под ред., Куприянов А.И. — Москва : КноРус, 2021. — 267 с. — ISBN 978-5-406-08259-1. — URL: https://book.ru

Дополнительные учебные издания

4. 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

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. 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

Интернет-ресурсы

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

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

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

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

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

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

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

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

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

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

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

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

Методические рекомендации для обучающихся по освоению дисциплины

19. Методические указания для обучающихся по выполнению практических работ.

20. Методические указания для обучающихся по выполнению заданий самостоятельной работы.