ДЕПАРТАМЕНТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ТОМСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТОМСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности:

10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Томск
2020 год

ОДОБРЕНО
Предметной (цикловой) комиссией
информационных технологий
Председатель
_____А.М. Вернигора
Протокол № 8
от «15 » июня 2020 г.

УТВЕРЖДАЮ
Зам. директора по УМР
_____ Л.В. Сидакова
от «29 » июня 2020 г.

Заведующий библиотекой
_____О.А Пинаева
от «22 » июня 2020 г.

Рабочая программа учебной дисциплины разработана на основе приказа Министерства образования и науки Российской Федерации от 09.12.2016 № 1551 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования» по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Организация-разработчик: ОГБПОУ «Томский индустриальный техникум»

Разработчики:

Федорова Татьяна Викторовна, преподаватель первой квалификационной категории

Маслова Екатерина Константиновна. преподаватель первой квалификационной категории

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
Организационно-правовое обеспечение информационной безопасности

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Дисциплина «Организационно-правовое обеспечение информационной безопасности» входит в состав профессионального цикла. Изучение дисциплины должно предшествовать изучению профессиональных модулей, входящих в состав ППССЗ.

1.3. Цель и планируемые результаты освоения дисциплины:

В результате освоения дисциплины обучающийся должен уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; применять основные правила и документы системы сертификации Российской Федерации; классифицировать основные угрозы безопасности информации.

В результате освоения дисциплины обучающийся должен знать: сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; источники угроз информационной безопасности и меры по их предотвращению; жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности.

В результате изучения дисциплины обучающийся осваивает элементы общих компетенций.

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
ОК 9.	Использовать информационные технологии в профессиональной деятельности.

В результате изучения дисциплины обучающийся осваивает элементы профессиональных компетенций

Код	**Наименование видов деятельности и профессиональных компетенций**
ПК 1.4.	Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Суммарная учебная нагрузка во взаимодействии с преподавателем	**98**
Самостоятельная работа[1]	-
Консультации	*6*
Объем образовательной программы	**92**
в том числе:	
теоретическое обучение	43
лабораторные работы (если предусмотрено)	-
практические занятия (если предусмотрено)	49
курсовая работа (проект) (если предусмотрено)	-
контрольная работа	-
Самостоятельная работа	-
Промежуточная аттестация проводится в форме *экзамена*	

Во всех ячейках со звездочкой (*) следует указать объем часов.

[1]) Самостоятельная работа в рамках примерной программы может быть не предусмотрена, при разработке рабочей программы вводится за счет вариативной части не более 20 процентов для профессий и не более 20 процентов для специальностей.

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	*Содержание учебного материала и формы организации деятельности обучающихся*	*Уровень освоения*	*Объем часов*	*Коды компетенций, формированию которых способствует элемент программы*
1	*2*		*3*	
Раздел 1	**Правовое обеспечение информационной безопасности**		**57**	
Тема 1.1. Введение в правовое обеспечение информационной безопасности	Основные правовые понятия. Источники права. Основы государственного устройства РФ. Информационная безопасность государства. Нормативные правовые акты Российской Федерации в области информации, информационных технологий и защиты информации. Конституционные права граждан на информацию и возможности их ограничения	2	2	ОК 02, ОК 03, ОК 06, ОК 09
Тема 1.2. Государственная система защиты информации в Российской Федерации, ее организационная структура и функции	Государственная система защиты информации в Российской Федерации, ее организационная структура и функции. Федеральная служба безопасности Российской Федерации, ее задачи и функции в области защиты информации и информационной безопасности. Федеральная служба по техническому и экспортному контролю, ее задачи, полномочия и права в области защиты информации	2	**4**	ОК 02, ОК 03, ОК 06

Тема 1.3 Информация как объект правового регулирования	Информация как объект правовых отношений. Субъекты и объекты правовых отношений в информационной сфере. Виды информации по законодательству Российской Федерации. Нормы законодательства Российской Федерации, определяющие защиту информации.	2	**4**	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09 ПК 2.4
	Консультация по разделу 1: Правовое обеспечение информационной безопасности	2	**2**	
	Практические занятия 1. Нормативные правовые акты в области информационной безопасности. 2. Нормативные методические документы в области защиты информации 3. Понятийный аппарат направления «Информационная безопасность» 4. Работа со справочно-поисковой системой «КонсультантПлюс» 5. Работа со справочно-поисковой системой «Гарант»	3	**10**	
Тема 1.4 Правовой режим защиты государственной тайны	Государственная тайна как особый вид защищаемой информации. Законодательство Российской Федерации в области защиты государственной тайны. Основные понятия, используемые в Законе Российской Федерации «О государственной тайне», и их определения. Степени секретности сведений, составляющих государственную тайну. Отнесение сведений к	2	**6**	ОК 01, ОК 02, ОК 03, ОК 06

	государственной тайне. Засекречивание и рассекречивание. Документирование сведений, составляющих государственную тайну. Реквизиты носителей сведений, составляющих государственную тайну. Допуск к государственной тайне и доступ к сведениям, составляющим государственную тайну. Органы защиты государственной тайны в Российской Федерации. Ответственность за нарушения правового режима защиты государственной тайны			
Тема 1.5 Правовые режимы защиты конфиденциальной информации	Законодательство Российской Федерации в области защиты конфиденциальной информации. Виды конфиденциальной информации по законодательству Российской Федерации. Отнесение сведений к конфиденциальной информации. Нормативно-правовое содержание Федерального закона «О персональных данных». Документирование сведений конфиденциального характера. Защита конфиденциальной информации. Ответственность за нарушение режима защиты конфиденциальной ин-формации.	1	**4**	ОК 02, ОК 03, ОК 06, ОК 09 ПК 2.4
	Практические занятия 6. Правовое регулирование и защита государственной тайны. 7. Правовые режимы защиты конфиденциальной информации. 8. Решение ситуационных задач.	3	**17**	
Раздел 2	**Лицензирование и сертификация в области защиты информации**		**30**	

Тема 2.1 Лицензирование деятельности в области защиты информации	Основные понятия в области лицензирования и их определения. Нормативные правовые акты, регламентирующие лицензирование деятельности в области защиты информации. Виды деятельности в области защиты информации, подлежащие лицензированию. Участники лицензионных отношений в области защиты информации. Порядок получения лицензий на деятельность в области защиты информации.	2	4	ОК 01, ОК 02, ОК 03, ОК 09, ПК 2.4, ПК 3.2, ПК 3.5
	Практические занятия: 9. Семинарское занятие: Изучение положений о государственном лицензировании деятельности в области защиты информации 10. Лицензирование в информационной сфере.	3	6	
Тема 2.2 Сертификация и аттестация по требованиям безопасности информации	Аттестация объектов информатизации по требованиям безопасности информации. Основные понятия в области аттестации по требованиям безопасности информации и их определения. Системы сертификации средств защиты информации по требованиям безопасности информации	2	2	ОК 1, ОК 2, ОК 3, ОК 9 ПК 2.4, ПК 3.2, ПК 3.5
	Консультация по разделу 2: Лицензирование и сертификация в области защиты информации	2	2	
	Практические занятия: 11. Семинарское занятие: Изучение положений о сертификации средств защиты информации по требованиям безопасности информации 12. Основные правила и документы системы сертификации Российской Федерации 13. Подготовки документов к сертификации 14. Подготовка документов к аттестации объектов		12	

	информатизации.			
Раздел 3	**Организационное обеспечение информационной безопасности**			
Тема 3.1 Допуск лиц и сотрудников к сведениям, составляющим государственную тайну и конфиденциальную информацию	Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией. Должности, составляющие с точки зрения защиты информации «группы риска». Понятие «допуск». Формы допусков, их назначение и классификация. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления, утверждения Работа по обучению персонала, допускаемому к конфиденциальной информации	2	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ПК 2.4
Тема 3.2 Организация пропускного и внут-риобъектового режимов	Понятие «охрана». Организация охраны территории, зданий, помещений и персонала. Цели и задачи охраны. Объекты охраны. Виды и способы охраны. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Понятие пропуска. Понятие внутриобъектового режима. Общие требования внутриобъектового режима Требования к помещениям, в которых ведутся работы с конфиденциальной информацией, конфиденциальные переговоры.	2	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 06, ПК 2.4,
Тема 3.3 Организация ремонтного обслуживания аппаратуры и средств защиты	Изъятие компьютерной техники и носителей информации. Инструкция изъятия компьютерной техники. Исследование компьютерной техники и носителей информации. Оформление результатов исследования	2	2	ОК 01, ОК 02, ОК 03, ПК 1.3, ПК 2.4, ПК 3.2, ПК 3.5
	Консультация по разделу 3: Организационное обеспечение информационной безопасности.	2	2	
Раздел 4	**Основы трудового права**			

Тема 4.1 Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения.	Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения. Понятие, стороны и содержание трудового договора. Виды трудовых договоров. Заключения трудового договора. Испытательный срок. Правовые гарантии в области оплаты труда.	1	4	ОК 02, ОК 03, ОК 04, ОК 06, ОК 09
	Практические занятия: 15. Составление трудового договора сотрудника службы информационной безопасности	2	4	
Итоговая аттестация в форме экзамена.			**3**	
Всего:			***98***	

По каждой теме описывается содержание учебного материала (в дидактических единицах), наименования необходимых лабораторных работ, практических и иных занятий, в том числе контрольных работ, а также тематика самостоятельной работы. Уровень освоения проставляется напротив дидактических единиц (отмечено двумя звездочками). Если предусмотрены курсовые проекты (работы) по дисциплине, приводится их тематика. Объем часов определяется по каждой позиции столбца 3 (отмечено звездочкой).

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Материально-техническое обеспечение

Реализация программы дисциплины требует наличия учебной аудитории № 401 кабинет Нормативного правового обеспечения информационной безопасности

Оборудование кабинета и рабочих мест кабинета Нормативного правового обеспечения информационной безопасности:

- Презентационное оборудование, проектор, полотно для проектора,

- ноутбук,

- учебная мебель.

- Учебно-наглядное пособие: комплект УМК по дисциплине (дидактические материалы, контрольно-оценочные средства, наглядные материалы и т.д.)

- Программное обеспечение: ОС Windows 10 education

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

Информационная безопасность : учебник / В.П. Мельников. под ред., А.И. Куприянов. —2-е изд., перераб. и доп. Москва : КноРус, 2020. — 267 с. — (Среднее профессиональное образование). ISBN 978-5-406-07382-7. — URL: https://book.ru/book/932059 (дата обращения: 26.06.2020). — Текст : электронный. Реком. ФГБОУ ВО «МГТУ «Станкин»

Электронные ресурсы

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Утвержден и введен в действие Приказом Федерального агенства по техническому регулированию и метрологии от 18 декабря 2008г. №532-ст. - Электронный фонд правовой и нормативно-технической документации «Консорциум КОДЕКС». - URL: (дата обращения 15.06.2020). – Режим доступа: свободный.

Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями) – информационно-поисковая система «Гарант» - URL: https://base.garant.ru/12148555/ (дата обращения 15.06.2020). – Режим доступа: свободный.

Интернет- ресурсы

Росстандарт - Федеральное агентство по техническому регулированию и метрологии . — URL: https://www.rst.gov.ru/portal/gost/search?query=информационная+безопасность (дата обращения: 26.06.2020). — Текст : электронный. – Режим доступа: свободный.

Роскомнадзор – сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций — URL: https://15.rkn.gov.ru/law/p8182/ (дата обращения: 24.06.2020). — Текст : электронный. – Режим доступа: свободный

3.3. Организация образовательного процесса

Курс предполагает проведение теоретических и практических занятий. Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе выполнения индивидуальных заданий, проведения практических. Промежуточная аттестация проводится в форме экзамена

3.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров наличие высшего образования

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
У.1 Классифицировать защищаемую информацию по видам тайны и степеням секретности; У.2 Классифицировать основные угрозы безопасности информации;	Оценка умений осуществляется по пятибалльной шкале	Контроль знаний и умений осуществляется в ходе выполнения практических и лабораторных работ, промежуточной аттестации. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы Экспертное заключение преподавателя
З.1 Сущность и понятие информационной безопасности, характеристику ее составляющих; З.2 Место информационной безопасности в системе национальной безопасности страны; З.3 Виды, источники и носители защищаемой информации; З.4 Источники угроз безопасности информации и меры по их предотвращению; З.5 Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; З.6 Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; З.7 Современные средства и способы обеспечения информационной безопасности; З.8 Основные методики анализа угроз и рисков	Оценка умений осуществляется по пятибалльной шкале	Контроль знаний и умений осуществляется в ходе выполнения практических и лабораторных работ, промежуточной аттестации. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы Экспертное заключение преподавателя

информационной безопасности.		

Оценка знаний, умений и навыков по результатам текущего контроля производится в соответствии с универсальной шкалой (таблица).

Процент результативности (правильных ответов)	Качественная оценка индивидуальных образовательных достижений	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	Отлично
80 ÷ 89	4	Хорошо
70 ÷ 79	3	Удовлетворительно
менее 70	2	Неудовлетворительно

5. *ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ В ДРУГИХ ПООП*

Учебная дисциплина ОПД 04 «Основы информационной безопасности» может быть использована для обучения укрупненной группы профессий и специальностей 10.00.00 «Информационная безопасность»