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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВЫ 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»

Разработчик:

Асадулина Галия Спартаковна, преподаватель высшей квалификационной категории

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
Основы информационной безопасности

1.1. Область применения программы

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

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: учебная дисциплина «Основы информационной безопасности» входит в общепрофессиональный цикл основной профессиональной образовательной программы

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.

Перечень общих компетенций, элементы которых формируются в рамках дисциплины

Код	Наименование общих компетенций
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.

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	**36**
Самостоятельная работа[1]	-
Консультации	-
Объем образовательной программы	**36**
в том числе:	
теоретическое обучение	18
лабораторные работы (если предусмотрено)	-
практические занятия (если предусмотрено)	18
курсовая работа (проект) (если предусмотрено)	-
контрольная работа	-
Самостоятельная работа	-
Промежуточная аттестация проводится в форме *дифференцированного зачета*	

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***	***Осваиваемые элементы компетенций***
1	***2***		***3***	
Раздел 1	***Теоретические основы информационной безопасности***		***22***	
Тема 1.1. Основные понятия и задачи информационной безопасности	*Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.* *Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.**	*1*	***2***	*ОК 3, ОК 6, ОК 9*
Тема 1.2. Основы защиты информации	*Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.* *Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.* *Цели и задачи защиты информации. Основные понятия в области защиты информации.* *Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности. Модель нарушителя**	*1*	***4***	*ОК 3, ОК 6, ОК 9*
	Практические занятия 1. *Информация и ее свойства. Компьютерное тестирование по теме «Основные понятия безопасности».** 2. *Рассмотрение и анализ Доктрины информационной безопасности*		***6***	*ОК 3, ОК 6, ОК 9*

	*Российской Федерации.** 3. *Определение объектов защиты на типовом объекте информатизации.**			
Тема 1.3. Угрозы информационной безопасности. Классификация угроз.	*Понятие угрозы безопасности информации Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации Уязвимости. Методы оценки уязвимости информации**	*1*	***4***	*ОК 3, ОК 6, ОК 9*
	Практические занятия 4. *Построение обобщенной модели способов несанкционированного доступа к источникам конфиденциальной информации. Классификация угроз. План защиты информационных ресурсов от несанкционированного доступа.** 5. *Оценка вероятных угроз информационной безопасности объекта.** 6. *Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)**		***6***	*ОК 3, ОК 6, ОК 9*
Раздел 2	***Методология защиты информации***		***14***	
Тема 2.1. Методологические подходы к защите информации	*Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.**	*1*	*2*	*ОК 3, ОК 6, ОК 9*
Тема 2.2. Нормативно правовое регулирование защиты информации	*Организационная структура системы защиты информации Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. **	*1*	*2*	*ОК 3, ОК 6, ОК 9, ОК10, ПК.2.3*
	Практические занятия: 7. *Обзор основных законодательных актов в сфере информационной безопасности. Компьютерное тестирование по теме «Основные понятия системы национальной безопасности»**		*2*	*ОК 3, ОК 6, ОК 9, ОК10,*
Тема 2.3. Тема 2.3. Защита	*Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в*	*1*	*2*	*ОК 3, ОК 6, ОК 9*

информации в автоматизированных (информационных) системах	*автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации.* *Комплекс организационных и технических средств защиты информации. Целостность и изменчивость при решении задачи обеспечения безопасности данных. Оценка надежности обеспечения защиты информации. Контроль и тестирование систем безопасности.* *Принципы формирования и функционирования службы безопасности предприятия.**			
	Практические занятия: *8. Выбор мер защиты информации для автоматизированного рабочего места* *Построение структурной схемы «Этапы организации системы защиты информации на предприятии». Презентация.**		*4*	*ОК 3, ОК 6, ОК 9*
Дифференцированный зачет в форме итогового компьютерного тестирования *******			***2***	*ОК 3, ОК 6, ОК 9, ОК10,*
Всего:			***36***	

Примечание: * - с использованием технологий дистанционного обучения.

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 ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация программы дисциплины требует наличия учебной аудитории № 405 «Лаборатория защиты информации от утечки по техническим каналам».

Оборудование лаборатории и рабочих мест лаборатории Защиты информации от утечки по техническим каналам:

- Презентационное оборудование,

- интерактивная панель,

- 12 ПК,

- учебная мебель.

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

- Программное обеспечение: ОС Linux Debian 10 (Лицензия GNU General Public License), ОС Windows 10 education

3.2. Информационное обеспечение обучения

Перечень используемых 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»

Интернет- ресурсы

Безопасность ПК| Защита компьютера| Информационная безопасность - URL: http://bezopasnostpc.ru// (дата обращения: 10.06.2020). — Текст : электронный. - Режим доступа: свободный

CISO CLUB – сайт Клуба информационной безопасности - URL: https://cisoclub.ru// (дата обращения: 10.06.2020). — Текст : электронный. - Режим доступа: свободный

3.3. Организация образовательного процесса

Изучение дисциплины должно следовать за изучением дисциплин «Математика» и «Информатика» и предшествовать изучению профессиональных модулей, входящих в состав ППССЗ. Курс предполагает проведение теоретических и практических занятий. Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и тестирования. Итоговый контроль (промежуточная аттестация) проводится в форме дифференцированного зачета

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 конфиденциальности; У.2 Применять основные правила и документы системы сертификации Российской Федерации; У.3 Классифицировать основные угрозы безопасности	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 Источники угроз информационной безопасности и меры по их предотвращению; З.4 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности	Оценка знаний 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

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*

Программа учебной дисциплины может быть использована для обучения укрупненной группы профессий и специальностей 10.00.00 «Информационная безопасность»

6. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Перечислите названия всех основных законов по защите информации с указанием их номеров.

2. Перечислите информацию, относящуюся к персональным данным физического лица.

3. Перечислите сведения, которые не могут быть отнесены к государственной и коммерческой тайне.

4. Проанализируйте возможные информационные потоки в перечисленных сферах деятельности на примере типовой организации.

5. Постройте модель угроз для заданного объекта исследования.

6. Постройте модель нарушителя для заданного объекта исследования.

7. Перечислите ряд сведений, которые согласно Указу Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера» носят конфиденциальный характер.

8. Что такое политика ИБ? К каким практическим шагам должно сводиться определение политики ИБ?

9. Дайте определение Доктрины информационной безопасности Российской Федерации.

10. Дайте определение понятию информационной безопасности РФ.

11. Перечислите основные составляющие комплексной системы защиты информации.

12. Назовите и прокомментируйте основные свойства информации, подлежащие защите.

13. Охарактеризуйте два основных рода (вида) информации.

14. Чем определяется ценность информации для владельца?

15. Что такое конфиденциальность информации, государственная и коммерческая тайна?

16. Какие три возможные степени секретности вы знаете?

17. Каковы три категории ценности коммерческой информации?

18. Что является предметом защиты в компьютерных сетях? Приведите особенности этого предмета.

19. Дайте определение и обоснование следующих понятий: «информационная система» и «информационная сфера», «информационное оружие», «информационная война», «информационная агрессия».

20. Какие существуют подходы к формированию и развитию научно-производственного потенциала информационной индустрии. Их достоинства и недостатки.

21. Перечислите основные органы, обеспечивающие национальную безопасность РФ.

22. Дайте определение сертификации применительно к средствам защиты информации.

23. Что входит в нормативную правовую базу системы сертификации? Назовите срок действия сертификата.

24. Расшифруйте аббревиатуру ФСТЭК и поясните, чем занимается данная организация.

25. Перечислите основные этапы жизненного цикла конфиденциальной информации.

26. Что такое угроза безопасности? Какие классы угроз вы знаете?

27. Перечислите основные источники угроз.

28. Перечислите пути противодействия нарушению конфиденциальности.

29. Перечислите комплекс организационных и технических средств защиты информации.

30. Перечислите принципы формирования и функционирования службы безопасности предприятия