Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КОЛЛЕДЖ КОСМИЧЕСКОГО МАШИНОСТРОЕНИЯ И ТЕХНОЛОГИЙ

УТВЕРЖДАЮ
Проректор по учебно-методической работе ГБОУ ВО МО «Технологический университет»
_____ Н.В. Бабина
«31» августа 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.12 Информационная безопасность

09.02.04 «Информационные системы (по отраслям)»

Базовой подготовки

Королев, 2020

Автор: Никонова Д.Н. Рабочая программа учебной дисциплины ОП.12 Информационная безопасность. – Королёв МО: «МГОТУ», 2020 - 18 **с.**

Рабочая программа учебной дисциплины составлена в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования (далее - ФГОС СПО) и учебного плана по специальности 09.02.04 «Информационные системы (по отраслям)».

Рабочая программа рассмотрена и одобрена на заседании цикловой комиссии по специальности 09.02.04 «Информационные системы (по отраслям)» 28.08.2020 г., протокол № 1.

Рабочая программа утверждена на заседании УМС ГБОУ ВО МО «Технологический университет» 31.08.2020 г., протокол № 1.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.12 Информационная безопасность является вариативной частью программы подготовки специалистов среднего звена по специальности 09.02.04 Информационные системы (по отраслям).

Рабочая программа учебной дисциплины ОП.12 Информационная безопасность может быть использована при реализации:

- программ дополнительного профессионального образования: повышения квалификации и переподготовке рабочих и специалистов среднего профессионального образования.

1.2. Общие и профессиональные компетенции, полученные в результате освоения учебной дисциплины

Техник по информационным системам должен обладать следующими **общими компетенциями**:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Техник должен обладать следующими **профессиональными компетенциями**:

ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы.

ПК 1.2. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

ПК 1.3. Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения.

ПК 1.9. Выполнять регламенты по обновлению, техническому сопровождению и восстановлению данных информационной системы, работать с технической документацией.

ПК 1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

1.3. Место учебной дисциплины в структуре основной профессиональной образовательной программы:

ОП.12 Информационная безопасность является вариативной частью программы подготовки специалистов среднего звена по специальности ***09.02.04 Информационные системы (по отраслям)*** и входит профессиональный цикл.

1.4. Цели и задачи учебной дисциплины– требования к результатам освоения учебной дисциплины:

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

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать основные угрозы безопасности информации;
- выбирать средства обеспечения информационной безопасности информационной системы предприятия;
- применять основные правила и документы системы сертификации Российской Федерации;
- использовать средства защиты данных от разрушающих программных воздействий, включая компьютерные вирусы;
- проводить базовые работы по профилактике нарушений информационной безопасности и построению защищенных информационных систем с использованием стандартных аппаратно-программных решений.

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

- проблемы защиты информации на предприятии;
- вопросы административного и нормативно-правового обеспечения защиты информации;
- 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 методы защиты информации в информационных системах.

1.5. Рекомендуемое количество часов на освоение рабочей программы учебной дисциплины:

максимальной учебной нагрузки обучающегося – 73 часа, в том числе:

обязательной аудиторной учебной нагрузки обучающегося – 46 часов;

самостоятельной работы обучающегося– 27 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	**73**
Обязательная аудиторная учебная нагрузка (всего), в том числе	**46**
лекции	*22*
практические занятия	*24*
Самостоятельная работа обучающегося (всего)	**27**
Итоговая аттестация в форме ***Дифференцированный зачет***	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, практические занятия и лабораторные работы, самостоятельная работа студента	Объем часов	Уровень освоения*
Раздел 1 Комплексный подход к обеспечению информационной безопасности			
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**		
	Основные понятия и задачи информационной безопасности. Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	2	
	Понятия угроза, нарушитель, риски информационной безопасности Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации.	2	
Тема 1.2. Основы защиты информации	**Содержание учебного материала**		
	Основы защиты информации. Понятия государственной тайны и конфиденциальной информации. Цели и задачи защиты информации. Основные понятия в области защиты информации государственной и конфиденциальной информации. Защищаемые свойства информации. Классификация информации по видам доступа. Понятие жизненного цикла конфиденциальной информации.	2	
	Основы защиты информации. Понятие системы менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности.	2	
	Практические занятия		
	Организация защиты информации, содержащей государственную тайну.	2	
	Организация защиты конфиденциальной информации на предприятии.	2	
	Этапы создания информационных систем предприятия, требования обеспечения	2	

Наименование разделов и тем	Содержание учебного материала, практические занятия и лабораторные работы, самостоятельная работа студента	Объем часов	Уровень освоения*
	информационной безопасности		
	Содержание политики информационной безопасности предприятия	2	
Тема 1.3. Угрозы безопасности защищаемой информации.	**Содержание учебного материала**		
	Угрозы безопасности защищаемой информации. Информационная система как объект защиты информации. Системная классификация угроз безопасности информации.	2	
	Защита информационной системы от несанкционированного доступа. Каналы и методы несанкционированного доступа к информации. Уязвимости информационных систем. Понятие модели нарушителя.	2	
	Практические занятия		
	Построение модели угроз и нарушителей информационной безопасности системы электронного документооборота предприятия	2	
Тема 1.4. Организация комплексной защиты информации	**Содержание учебного материала**		
	Организация комплексной защиты информации. Законодательный уровень информационной безопасности. Значимость уровня в комплексном подходе. Меры законодательного уровня. Законодательная и нормативно – правовая база РФ в области информатизации и защиты информации. Ответственность за нарушение законодательства в информационной сфере.	2	
	Практические занятия		
	Изучение основных законов РФ в области информационной безопасности.	2	
	Административный уровень информационной безопасности. Политика и программа безопасности.	2	
	Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание	2	

Наименование разделов и тем	Содержание учебного материала, практические занятия и лабораторные работы, самостоятельная работа студента	Объем часов	Уровень освоения*
	работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.		
	Программно-технический уровень информационной безопасности. **Основные понятия и меры уровня.** Особенности современных информационных систем. Архитектурная безопасность.	2	
Раздел 2 Методы и средства обеспечения безопасности информации			
Тема 2.1. Защита информации от утечки по техническим каналам	**Содержание учебного материала**		
	Защита информации от утечки по техническим каналам. Основные виды технических каналов утечки информации. Техника промышленного шпионажа. Противодействие наблюдению. Противодействие прослушиванию. Методы и средства защиты от побочных электромагнитных излучений и наводок.	2	
Тема 2.2. Защита информации от несанкционированного доступа	**Содержание учебного материала**		
	Защита информации от несанкционированного доступа. Характеристика средств защиты информации в компьютерных системах от несанкционированного доступа. Идентификация и аутентификация пользователей: основные понятия, парольная аутентификация, виды паролей, биометрическая аутентификация. Управление доступом: основные понятия, виды разграничения доступа, особенности дискреционного, мандатного и ролевого управления доступом Защита программных средств от несанкционированного копирования и исследования. Протоколирование и аудит: основные понятия, активный аудит.	2	
	Практические занятия		
	Документы Гостехкомиссии России по защите информации. Изучение методов аутентификации, использующие пароли. Построение системы разграничения доступа в базе данных на основе ролевой модели.	2	
	Общая характеристика компонентов системы защиты операционной системы Windows. Изучение политики безопасности операционной системы Windows.	2	

Наименование разделов и тем	Содержание учебного материала, практические занятия и лабораторные работы, самостоятельная работа студента	Объем часов	Уровень освоения*
Тема 2.3. Криптографические методы защиты информации	**Содержание учебного материала**		
	Криптографические методы защиты информации. Понятие криптографической защиты информации. Классификация криптографических средств. Методы шифрования. Функция хэширования. Электронная цифровая подпись и ее применение для контроля целостности программ и данных.	2	
Тема 2.4. Компьютерные вирусы и средства антивирусной защиты	**Содержание учебного материала**		
	Компьютерные вирусы и средства антивирусной защиты. Общие сведения о компьютерных вирусах. Классификация компьютерных вирусов. Основные каналы распространения вирусов. Вредоносные программы и их классификация. Методы и средства защиты от компьютерных вирусов. Методы обнаружения и удаления вирусов. Профилактика заражения вирусами компьютерных систем. Программные закладки и методы защиты от них. Антивирусные программные комплексы.	2	
	Практическое занятие		
	Знакомство с антивирусными программными комплексами. Восстановление зараженных файлов. Профилактика проникновения «троянских программ».	2	
Всего аудиторных часов		46	
Самостоятельная работа обучающегося		27	
	Всего	**73**	

*Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует кабинета информатики и информационных технологий.

Оборудование кабинета:

- сетевое АРМ преподавателя;
- доска маркерная;
- компьютерные станции
- необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением;
- проектор;
- принтер;
- сканер.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2018. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз.
2. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с. — (Среднее профессиональное образование)

Дополнительные источники:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2018. - 222 с. - ISBN 978-5-369-01178-2 - Текст : электронный.
2. Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.: 60х90 1/16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-369-01761-6

Интернет ресурсы:

1. Библиотека // Единое окно доступа к образовательным ресурсам: информационная система [Электронный ресурс].–Режим доступа: http://window.edu.ru/window/library?p_rubr=2.2.75.6.10
2. Интеллектуальная система Cisco [Электронный ресурс]. – Режим доступа: http://www.cisco.com/web/RU/index.html
3. Российское образование: федеральный портал [Электронный ресурс]. – Режим доступа: http://www.edu.ru
4. Федеральный центр информационно-образовательных ресурсов [Электронный ресурс]. – Режим доступа: http://fcior.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	1. Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы.
классифицировать основные угрозы безопасности информации;	1. Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы.
выбирать средства обеспечения информационной безопасности информационной системы предприятия	1. Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы.
использовать средства защиты данных от разрушающих программных воздействий, включая компьютерные вирусы	1. Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы. 2. Текущий контроль в форме: - защиты практических работ; - отчёта по проделанной внеаудиторной самостоятельной работе; - индивидуальный и фронтальный опрос в ходе аудиторных занятий.
проводить базовые работы по профилактике нарушений информационной безопасности и построению защищенных информационных систем с использованием стандартных аппаратно-программных решений.	1. Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы. 2. Текущий контроль в форме: - защиты практических работ; - отчёта по проделанной внеаудиторной самостоятельной работе; - индивидуальный и фронтальный опрос в ходе аудиторных занятий.
Знания:	

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
вопросы административного и нормативно-правового обеспечения защиты информации	1.Наблюдение за деятельностью обучающегося в процессе освоения образовательной программы. 2. Текущий контроль в форме индивидуального и фронтального опроса в ходе аудиторных занятий. 3. Итоговая аттестация в форме дифференцированного зачета.
основные системы защиты информации в России и в ведущих зарубежных странах	1. Текущий контроль в форме индивидуального и фронтального опроса в ходе аудиторных занятий. 2. Итоговая аттестация в форме дифференцированного зачета.
современные средства и методы защиты информации в информационных системах	1. Текущий контроль в форме индивидуального и фронтального опроса в ходе аудиторных занятий. 2. Итоговая аттестация в форме дифференцированного зачета.

4.1. Перечень вопросов, выносимых на экзамен по учебной дисциплине

1. Комплексный подход к обеспечению информационной безопасности
2. Понятие и составляющие информационной безопасности
3. Угрозы информационной безопасности в компьютерных системах
4. Законодательный уровень информационной безопасности
5. Административный уровень информационной безопасности
6. Процедурный уровень информационной безопасности
7. Программно-технический уровень информационной безопасности
8. Методы и средства обеспечения безопасности информации
9. Защита информации от утечки по техническим каналам
10. Защита информации от несанкционированного доступа

11. Криптографические методы защиты информации

12. Компьютерные вирусы и средства антивирусной защиты

13. Вирусы как угроза ИБ

14. Средства антивирусной защиты

15. Стандарты защищенности информации в компьютерных системах

16. Стандарты и спецификации в области информационной безопасности

4.2. Критерии оценки ответов

При оценке ответов дополнительно должны быть учтены качество сообщения, отражающего основные моменты и ответы на вопросы, заданные по теме вопроса.

Результаты защиты определяются оценками *«отлично», «хорошо», «удовлетворительно», «неудовлетворительно».*

1. Оценки ***«отлично»*** заслуживает ответ, в котором полно и всесторонне раскрыто теоретическое содержание темы, дан глубокий критический анализ действующей практики учетно-аналитической работы. Студент при ответе дал аргументированные ответы на все вопросы преподавателя, проявил творческие способности в понимании и изложении ответов на вопросы.

2. Оценка ***«хорошо»*** выставляется за ответ, который имеет убедительный ответ. При его этом студент показывает знания вопросов темы, оперирует данными, вносит предложения по теме ответа, во время ответа использует наглядные пособия, без особых затруднений отвечает на поставленные вопросы.

3. Оценка ***«удовлетворительно»*** выставляется за ответ, в котором имеются замечания по содержанию ответа и методике анализа. В теоретических, выводы в основном правильные, предложения представляют интерес, но недостаточно убедительно аргументированы и не на все вопросы студент дал правильные ответы.

4. Оценка ***«неудовлетворительно»*** выставляется за ответ, который в основном отвечает предъявляемым вопросам, но студент не дал правильных ответов на большинство заданных вопросов, т.е. обнаружил серьезные пробелы в профессиональных знаниях.