

Государственное автономное профессиональное
образовательное учреждение Тюменской области
«Тюменский колледж транспортных технологий и сервиса»
(ГАПОУ ТО «ТКТТС»)

СОГЛАСОВАНО

Главный инженер,
железнодорожная станция Войновка-
структурное подразделение
Свердловской дирекции управления
движением
Центральной дирекции управления
движением –
филиала ОАО «РЖД»

Лазоренко А.В.

«28» апреля 2021 г.

М.П.



УТВЕРЖДАЮ

Заместитель директора
по учебно - производственной
работе

 Н.Ф. Борзенко

«28» апреля 2021 г.

РАБОЧАЯ ПРОГРАММА

учебная дисциплина ОП.12 Основы информационной безопасности
(вариативная часть)

специальность 23.02.01 Организация перевозок и управление на транспорте
(по видам) (базовая подготовка)

Рабочая программа учебной дисциплины ОП.12 Основы информационной безопасности разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальностям 23.02.01 Организация перевозок и управление на транспорте (по видам) и 23.02.06 Техническая эксплуатация подвижного состава железных дорог.

Рассмотрена на заседании ПЦК преподавателей дисциплин профессионального цикла автоматизации и информатики протокол № 9 от «21» апреля 2021 г.

Председатель ПЦК  /Колотыгина А.В./

Организация – разработчик: ГАПОУ ТО «ТКТТС»

Разработчик: Раемгулова Наталья Анатольевна, преподаватель первой квалификационной категории ГАПОУ ТО «ТКТТС».

СОДЕРЖАНИЕ

1.	Общая характеристика рабочей программы учебной дисциплины	4
2.	Структура и содержание учебной дисциплины	6
3.	Условия реализации рабочей программы учебной дисциплины	9
4.	Контроль и оценка результатов освоения учебной дисциплины	11

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОПЦ.02 АРХИТЕКТУРА АППАРАТНЫХ СРЕДСТВ»

1.1 Место дисциплины в структуре основной профессиональной образовательной программы.

Дисциплина ОП.12 Основы информационной безопасности входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

1.2 Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания, общие и профессиональные компетенции

Код ПК, ОК	Умения	Знания
ОК 03, ОК 06, ОК 09, ПК 2.2	<ul style="list-style-type: none">- классифицировать защищаемую информацию по видам тайны и степеням секретности;- классифицировать основные угрозы безопасности информации.	<ul style="list-style-type: none">- 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.

Освоение учебной дисциплины направлено на развитие общих и профессиональных компетенций, предусмотренных ФГОС по данным специальностям:

Код	Наименование общих компетенций
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ПК 2.2	Обеспечивать безопасность движения и решать профессиональные задачи посредством применения нормативно-правовых документов.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	52
в том числе:	
теоретическое обучение	30
лабораторные работы	-
практические занятия	6
курсовая работа (проект)	-
контрольная работа	-
<i>Самостоятельная работа</i>	16
Промежуточная аттестация (другая форма контроля)	

2.2 Тематический план и содержание учебной дисциплины «ОП.12 Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1 Тема 1.1. Основные понятия и задачи информационной безопасности	Теоретические основы информационной безопасности Содержание учебного материала 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.	22	ОК 03, ОК 06, ОК 09, ПК.2.2
	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.	6	ОК 03, ОК 06, ОК 09, ПК.2.2
	Практические занятия Определение объектов защиты на типовом объекте информатизации. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	2	
	Содержание учебного материала		

Тема 1.3. Угрозы безопасности защищаемой информации.	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации	6	ОК 03, ОК 06, ОК 09, ПК.2.2
	Практические занятия	2	
Раздел 2	Методология защиты информации	14	
Тема 2.1. Методологические подходы к защите информации	Содержание учебного материала	4	ОК 03, ОК 06, ОК 09, ПК.2.2
	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.		
Тема 2.2. Нормативно правовое регулирование защиты информации	Содержание учебного материала	4	ОК 03, ОК 06, ОК 9
	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. Основные правила и документы системы сертификации РФ в области защиты информации		
Тема 2.3. Защита информации в автоматизированных (информационных) системах	Содержание учебного материала	4	ОК 03, ОК 06, ОК 09
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутри объектовый режим. Принципы построения организационно-распорядительной системы.		
	Практические занятия	2	
	Выбор мер защиты информации для автоматизированного рабочего места		
	Самостоятельная работа обучающихся	16	
	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности. Подготовка к практическим работам с использованием методических рекомендаций преподавателя.	16	
Всего:		52	

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.12 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

3.1 Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория «Информационных ресурсов»:

- Рабочее место преподавателя (1)
- Посадочные места по количеству обучающихся (25)

Технические средства обучения:

– Автоматизированные рабочие места на 12 обучающихся (процессор Intel Core i5 3330 2.7 Ghz, ОЗУ 6 Gb, OS Windows 10x64);

– Автоматизированное рабочее место преподавателя (процессор Intel Core i5 3330 2.7 Ghz, ОЗУ 6 Gb, OS Windows 10x64);

– Комплект компьютерных комплектующих для производства сборки, разборки и сервисного обслуживания ПК и оргтехники (12);

– Специализированная мебель для сервисного обслуживания ПК с заземлением и защитой от статического напряжения;

– Проектор (1);

– Экран (1);

– Магнитно-маркерная доска (1);

Программное обеспечение общего и профессионального назначения:

- Arduino IDE; Eclipse IDE for Java Developers; Microsoft Visual Studio, Microsoft Windows 7, Microsoft Office 2010, Антивирус, Adobe Reader, Notepad++, Krita, Git, GIMP, Windjview, Audacity, PascalABS.

3.2 Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

3.2.1 Печатные издания

1. Бубнов А.А., Пржегорлинский В. Н., Савинкин О. А., Основы информационной безопасности (2-е изд.), М. Академия, 2019

3.2.2 Электронные издания (электронные ресурсы)

1. Вопросы кибербезопасности. Научный, периодический, информационнометодический журнал с базовой специализацией в области информационной безопасности. URL: <http://cyberrus.com/>
2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>
3. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
4. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
5. Образовательные порталы по различным направлениям образования и тематике <http://depoobr.gov35.ru/>
6. Справочно-правовая система «Консультант Плюс» www.consultant.ru
7. Справочно-правовая система «Гарант» www.garant.ru
8. Федеральный портал «Российское образование» www.edu.ru
9. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>

10. Российский биометрический портал www.biometrics.ru
11. Федеральный портал «Информационно- коммуникационные технологии в образовании» [http\:\: www.ict.edu.ru](http://www.ict.edu.ru)
12. Сайт Научной электронной библиотеки www.elibrary.ru

3.2.3 Дополнительные источники:

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ, 2019
<https://znanium.com/catalog/product/987215>
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2018. <https://znanium.com/catalog/product/957144>
3. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD): учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М. : КНОРУС, 2017. <http://znanium.com/catalog/product/763644>
4. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2018.
[http://biblioclub.ru/index.php?
page=book&id=571750](http://biblioclub.ru/index.php?page=book&id=571750)

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.12 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Результаты обучения	Критерии оценки	Методы оценки
Перечень знаний и умений, осваиваемых в рамках дисциплины:		
<p>Знания:</p> <ul style="list-style-type: none"> - сущность и понятие информационной безопасности, характеристику ее составляющих; <input type="checkbox"/> место информационной безопасности в системе национальной безопасности страны; - виды, источники и носители защищаемой информации; <input type="checkbox"/> 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; <input type="checkbox"/> современные средства и способы обеспечения информационной безопасности; <input type="checkbox"/> основные методики анализа угроз и рисков информационной безопасности. <p>Умения:</p> <ul style="list-style-type: none"> - классифицировать защищаемую информацию по видам тайны и степеням секретности; - классифицировать основные угрозы безопасности информации. 	<p>Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.</p> <p>Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности.</p>	<p>Устный опрос Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий.</p>