

РОСЖЕЛДОР
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный университет путей сообщения»(ФГБОУ ВО
РГУПС)
Тамбовский техникум железнодорожного транспорта(ТаТЖТ-филиал
РГУПС)



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Специальность: 09.02.11 Разработка и управление программным обеспечением

Тамбов

2026

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.11 Разработка и управление программным обеспечением

Организация-разработчик: Тамбовский железнодорожный техникум – филиал РГУПС

Разработчик: Михалина М.Л. преподаватель, первая категория

Рецензенты:

Кривенцова С. А. – преподаватель высшей категории ТаТЖТ- филиала РГУПС

Касатонов И.С. - Проректор по цифровой трансформации федерального государственного бюджетного образовательного учреждения высшего образования «Тамбовский государственный технический университет»

Рекомендована предметной (цикловой) комиссией специальности 09.02.01
Компьютерные системы и комплексы

Протокол № 09 от 16.02.2026 г

Председатель цикловой комиссии



Кривенцова С.А.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	4
1.1 Область применения программы.....	4
1.2. Цель и место дисциплины в структуре образовательной программы.....	4
1.3. Планируемые результаты освоения дисциплины.....	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....	8
2.1. Трудоемкость освоения дисциплины.....	8
2.2 Тематический план и содержание дисциплины.....	9
3 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ..	12
3.1 Требования к минимальному материально-техническому обеспечению	12
3.2 Информационное обеспечение обучения	12
4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ Error! Bookmark not defined.	
4.1 Контроль и оценка результатов освоения дисциплины Error! Bookmark not defined.	

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1 Область применения программы

Рабочая программа дисциплины (далее рабочая программа) является частью основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена. Рабочая программа разработана в соответствии с ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением

1.2. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «Основы информационной безопасности»: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Дисциплина «Основы информационной безопасности» включена в обязательную часть общепрофессионального цикла образовательной программы.

1.3. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ПОП).

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК.01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы	-

	<p>решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)</p>	<p>работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности</p>	
ОК.02	<p>определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач</p>	<p>номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.</p>	-
ОК.09	<p>понимать тексты на базовые профессиональные темы</p>	<p>лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности</p>	-
ПК 1.1	-	<p>принципы безопасности хранения данных</p>	-
ПК 1.4	-	<p>методы защиты баз данных от внешних угроз</p>	-
ПК 1.5	<p>шифровать данные и обеспечивать их</p>	<p>принципы криптографии и методов шифрования данных</p>	-

	конфиденциальность	стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.	
ПК 3.1	-	отраслевая нормативная техническая документация источники информации, необходимой для профессиональной деятельности	-
		современный отечественный и зарубежный опыт в профессиональной деятельности	-
ПК 3.2	-	принципы и методы обеспечения безопасности информационных систем	-
ПК 3.3	анализ требований безопасности информационных систем	принципов безопасности информационных систем современных методов и технологий в области безопасности информационных систем законодательных и нормативных актов в области безопасности информационных систем	применение современных методов и технологий в области безопасности информационных систем
ПК 3.5	-	источники угроз информационной безопасности и меры по их предотвращению	-
ПК 3.7	разрабатывать и реализовывать меры безопасности реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	основные угрозы безопасности мобильных приложений принципы криптографии и шифрования данных. стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA основные принципы	использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные. применение механизмов хеширования для

		<p>безопасности информации и методов ее защиты. стандартные криптографические алгоритмы для шифрования данных принципы обеспечения безопасности передачи данных по сети основы безопасности приложений и инфраструктуры методы анализа на уязвимости и мониторинга безопасности знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы</p>	<p>защиты паролей пользователей от несанкционированного доступа. обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS соблюдение законодательства и регуляций в области защиты данных</p>
--	--	---	--

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	Объем часов
Максимальная учебная нагрузка (всего)	52
Контактная нагрузка	32
в том числе:	
практические занятия	16
Самостоятельная работа обучающегося (всего)	20
Промежуточная аттестация в форме зачета	

2.2 Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, ак. ч /в том числе в форме практической подготовки, ак. ч	Коды компетенций и личностных результатов ²³ , формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Основы информационной безопасности (32 часа)			
Тема 1.1. Введение в информационную безопасность	Содержание		ОК 01 ОК 02 ПК 1.1 ПК 2.1 ПК 2.2
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности. Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности.	2	
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.2. Криптография	Содержание учебного материала		ОК 01 ОК 02 ПК 1.1 ПК 2.1 ПК 2.2
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	
	В том числе практических и лабораторных занятий		
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	2	
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.3. Защита сетевой инфраструктуры	Содержание		ОК 01 ОК 02 ПК 1.1 ПК 2.1 ПК 2.2
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	2	
	В том числе практических и лабораторных занятий		
	Организация защиты от атак		

	Организация работы VPN и межсетевое экрана	4	
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.4. Безопасность приложений	Содержание		
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	
	В том числе практических и лабораторных занятий		
	Тестирование на проникновение и анализ уязвимостей.	2	
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.5. Защита данных	Содержание		
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	2	
	В том числе практических и лабораторных занятий		
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным	2	
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.6. Безопасность облачных технологий	Содержание		
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	2	
	В том числе практических и лабораторных занятий		
	Изучение модели облачных услуг и их безопасности	2	
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.7. Инциденты безопасности	Содержание		
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	2	
	В том числе практических и лабораторных занятий		
	Работа с инцидентами.	2	
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.8. Социальная	Содержание		

инженерия и человеческий фактор	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	2	
	В том числе практических и лабораторных занятий		
	Разработка политики информационной безопасности	2	
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Промежуточная аттестация			

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1– ознакомительный (узнавание ранее изученных объектов, свойств);

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

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

3 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Учебно административный корпус, №412

Лаборатория программирование

Перечень основного оборудования Лаборатории программирование

1 Стол компьютерный СК -03 – 14 шт

Стол преподавателя -1 шт

Стул ученический 16 шт

Доска аудиторная 1 шт

Компьютер Pentium -13 шт

Плазменный телевизор Samsung – 1шт

Система программирования Visual C++2005 1 шт

Тематические плакаты 5 шт.

Учебно методический комплекс

3.2 Информационное обеспечение обучения

Основная

1. Внуков, А. А. Основы информационной безопасности: защита информации [Электронный ресурс]: учебное пособие для СПО /А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — Режим доступа: <https://urait.ru/bcode/>

2. Казарин, О. В. Надежность и безопасность программного обеспечения [Электронный ресурс]: учебное пособие для СПО / О. В. Казарин, И. Б. Шубинский.

– 2-е изд., испр. и доп.— Москва: Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — Режим доступа: <https://urait.ru/bcode/>

3. Щербак, А. В. Информационная безопасность [Электронный ресурс]: учебник для СПО / А. В. Щербак. – 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). —
— Режим доступа: <https://urait.ru/bcode/>

Дополнительная

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под ред. Т. А. Поляковой, А. А. Стрельцова. – 2-е изд., перераб. и доп.— Москва: Издательство Юрайт, 2026. — 357 с. — (Профессиональное образование). — Режим доступа: <https://urait.ru/bcode/>

2. Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум для СПО / С. А. Нестеров. — Москва: Издательство Юрайт, 2022. — 321 с. — (Профессиональное образование). - Режим доступа: <https://urait.ru/bcode/>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоённости компетенций	Методы оценки
<p>Знает:</p> <ul style="list-style-type: none"> - актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности 	<p>Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить;</p> <p>Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте;</p> <p>Знает алгоритмы выполнения работ в профессиональной и смежных областях;</p> <p>Знает методы работы в профессиональной и смежных сферах;</p> <p>Знает структуру плана для решения задач;</p> <p>Может произвести оценку результатов решения задач профессиональной деятельности</p> <p>Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности;</p> <p>Знает приемы структурирования информации;</p> <p>Знает формат оформления результатов поиска информации, современные средства и устройства информатизации;</p> <p>Может применять современные средства и устройства информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;</p>	<p>Экспертное наблюдение выполнения практических работ и видов работ по практике</p> <p>Диагностика (тестирование, контрольные работы)</p>

<p>в том числе с использованием цифровых средств;</p> <ul style="list-style-type: none"> - лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; - принципы безопасности хранения данных; - методы защиты баз данных от внешних угроз - принципы криптографии и методов шифрования данных; - стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; - методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; - отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; - современный отечественный и зарубежный опыт в профессиональной деятельности; - принципы и методы обеспечения безопасности информационных систем; - принципы безопасности информационных систем; - современные методы и технологии в области безопасности информационных систем; 	<p>Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности;</p> <p>Знает принципы безопасности хранения данных;</p> <p>Владеет методами защиты баз данных от внешних угроз</p> <p>Знает принципы криптографии и методов шифрования данных;</p> <p>Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.;</p> <p>Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных</p> <p>законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;</p> <p>Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности;</p> <p>Знает современный отечественный и зарубежный опыт в профессиональной деятельности;</p> <p>Владеет принципами и методами обеспечения безопасности информационных систем;</p> <p>Знает принципы безопасности информационных систем;</p> <p>Владеет современными методами и технологиями в области безопасности информационных систем;</p> <p>Знает законодательные и нормативные акты в области безопасности информационных систем;</p> <p>Знает источники угроз информационной безопасности и</p>	
---	--	--

<ul style="list-style-type: none"> - законодательные и нормативные акты в области безопасности информационных систем; - источники угроз информационной безопасности и меры по их предотвращению; - основные угрозы безопасности мобильных приложений; - принципы криптографии и шифрования данных; - стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; - законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - основные принципы безопасности информации и методов ее защиты; - стандартные криптографические алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети; - основы безопасности приложений и инфраструктуры; - методы анализа на уязвимости и мониторинга безопасности; - знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; 	<p>меры по их предотвращению;</p> <p>Имеет представление об основных угрозах безопасности мобильных приложений;</p> <p>Ориентируется в принципах криптографии и шифрования данных;</p> <p>Знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;</p> <p>Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;</p> <p>Владеет основными принципами безопасности информации и методов ее защиты;</p> <p>Знает стандартные криптографические алгоритмы для шифрования данных;</p> <p>Имеет представление о принципах обеспечения безопасности передачи данных по сети;</p> <p>Знает основы безопасности приложений и инфраструктуры;</p> <p>Знает методы анализа на уязвимости и мониторинга безопасности;</p> <p>Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений;</p> <p>Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения;</p> <p>Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.</p> <p>Может распознавать задачу и/или проблему в профессиональном и/или</p>	
---	---	--

<p>- знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.</p> <p>Умеет:</p> <ul style="list-style-type: none"> -распознавать задачу и/или проблему в профессиональном и/или социальном контексте; -анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; -составлять план действия; - определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); - определять задачи для поиска информации; - определять необходимые источники информации; - планировать процесс поиска; - структурировать получаемую информацию; - выделять наиболее значимое в перечне информации; - оценивать практическую 	<p>социальном контексте;</p> <p>Анализирует задачу и/или проблему и может выделить её составные части;</p> <p>Умеет определять этапы решения задачи;</p> <p>Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;</p> <p>Составляет план действия;</p> <p>Может определять необходимые ресурсы;</p> <p>Владеет актуальными методами работы в профессиональной и смежных сферах;</p> <p>Может реализовывать составленный план;</p> <p>Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника);</p> <p>Умеет определять задачи для поиска информации;</p> <p>Умеет определять необходимые источники информации;</p> <p>Планирует процесс поиска;</p> <p>Умеет структурировать получаемую информацию;</p> <p>Может выделить наиболее значимое в перечне информации;</p> <p>Умеет оценивать практическую значимость результатов поиска;</p> <p>Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач;</p> <p>Может использовать современное программное обеспечение;</p> <p>Может использовать различные цифровые средства для решения профессиональных задач;</p>	
---	---	--

<p>значимость результатов поиска;</p> <ul style="list-style-type: none"> - оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; - использовать современное программное обеспечение; - использовать различные цифровые средства для решения профессиональных задач; - понимать тексты на базовые профессиональные темы; - шифрование данных и обеспечивает их конфиденциальность; - анализировать требования безопасности информационных систем; - разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию. 	<p>Понимает тексты на базовые профессиональные темы;</p> <p>Умеет шифровать данные и обеспечивать их конфиденциальность;</p> <p>Умеет анализировать требования безопасности информационных систем;</p> <p>Может разрабатывать и реализовывать меры безопасности;</p> <p>Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.</p>	
--	--	--