Частное учреждение
профессиональная образовательная организация
ТЕХНИКУМ «БИЗНЕС И ПРАВО»

Утверждаю

Директор техникума

_____Д.К. Скрыльников

«27» августа 2026 г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.13 Основы информационной безопасности

для специальности
09.02.07 Информационные системы и программирование

Квалификация: разработчик веб и мультимедийных приложений

Объём дисциплины – 88 часов

Белореченск 2026 г.

Рабочая программа учебной дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.07 «Информационные системы и программирование» (утвержден приказом Минобрнауки России от 09.12.2016 №1547, с изменениями приказа Минпросвещения России от 17.12.2020 №747) и Программой подготовки специалистов среднего звена по специальности 09.02.07, разработанной ЧУПОО ТЕХНИКУМ «БИЗНЕС И ПРАВО».

Разработчики рабочей программы: Сурин А. Ю. – преподаватель информационных дисциплин ЧУПОО ТЕХНИКУМ «БИЗНЕС И ПРАВО»

Рецензенты:

Косяченко Н. П. – преподаватель высшей категории технических дисциплин ЧУПОО ТЕХНИКУМ «БИЗНЕС И ПРАВО»

Обсуждено и одобрено:

цикловой комиссией технических дисциплин протокол № 1 от «27» августа 2026 г.

Председатель цикловой комиссии _____ Н.А.Макаркова

Рассмотрено и рекомендовано к использованию в учебном процессе педагогическим советом от «27» августа 2026 г., протокол № 1

Заместитель директора
по методической работе _____ А.Н.Истомина

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.13. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 4

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 5

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ 9

4. ПЕЧАТНЫЕ И ЭЛЕКТРОННЫЕ ИЗДАНИЯ 10

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ 11

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.13. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Основы информационной безопасности» принадлежит к общепрофессиональному циклу. Дисциплина формирует базовые знания и умения в области защиты информации и является обязательной частью общепрофессионального цикла подготовки по специальности 09.02.07 Информационные системы и программирование.

1.2. Цель и планируемые результаты освоения дисциплины:

Формирование у обучающихся базовых знаний и практических умений в области информационной безопасности для защиты информационных ресурсов в ИТ-системах, а также навыков применения нормативно-правовой базы информационной безопасности.

Код ОК/ПК	Умения	Знания
ОК 01	Определять уровень угроз информационной безопасности; оценивать риски для информационных систем	Основные понятия, цели и задачи защиты информации; классификация угроз ИБ; источники возникновения угроз
ОК 02	Проводить сбор и анализ информации о потенциальных угрозах; оценивать защитные меры	Методы выявления угроз; средства мониторинга и анализа рисков
ОК 05	Разрабатывать и оформлять отчёты и инструкции по ИБ; составлять рекомендации	Правила оформления и документирования мер защиты информации
ОК 09	Использовать ИТ-средства для реализации мер информационной безопасности	Современные средства защиты информации; криптографические методы; системы аутентификации, логирования, резервного копирования
ПК 5.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием	Настройка аутентификации, шифрования, резервного копирования, мониторинга безопасности, защита веб-приложений
ПК 5.6	Разрабатывать техническую документацию на эксплуатацию информационной системы	Состав, структура и оформление технической документации по ИБ

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы дисциплины	***88***
Основное содержание	***78***
в том числе:	
теоретическое обучение (в том числе промежуточная аттестация)	40
практические занятия	30
Самостоятельные работы обучающегося	8
Консультации	4
Экзамен	**6**
ИТОГО	**88**

2.2 Тематический план и содержание учебной дисциплины
ОП.13. «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Наименование разделов и тем	Содержание учебного материала (основное и профессионально-ориентированное), лабораторные и практические занятия, прикладной модуль (при наличии)	Объем часов	Коды компетенции, формированию которых способствует элемент программы
1	2	3	4
	Раздел 1. Борьба с угрозами несанкционированного доступа	***32***	
Тема 1.1. Актуальность проблемы обеспечения информационной безопасности	**Содержание учебного материала**	***14***	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 5.6
	1. Основные понятия объекты, цели и задачи информационной безопасности. Основные понятия информационной безопасности. Угрозы информационной безопасности: классификация, источники возникновения. Анализ рисков информационной безопасности. Обеспечение информационной безопасности в ведущих зарубежных странах		
	В том числе, практических занятий:	***6***	
	Практическое занятие №1 «Анализ угроз веб-приложений и пользовательских данных»	*2*	
	Практическое занятие №2 «Жизненные циклы конфиденциальной информации»	*2*	
	Практическое занятие №3 «Элементы процесса менеджмента ИБ»	*2*	
Тема 1.2. Виды мер обеспечения информационной безопасности	**Содержание учебного материала**	***18***	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 5.6
	1. Виды мер обеспечения информационной безопасности. Мероприятия по защите информации. Виды и характеристики современных средств защиты. Аспекты, относящиеся к средствам защиты: аппаратные ключи, лицензирование, метод авторизации		
	В том числе, практических занятий:	***8***	
	Практическое занятие №4 «Разработка и внедрение политики безопасности для веб-приложений»	*2*	

	Практическое занятие №5 «Классификация защищаемой информации и хэширование паролей с использованием bcrypt/argon2»	*2*	
	Практическое занятие №6 «Внедрение паролей и двухфакторной аутентификации»	*2*	
	Практическое занятие №7 «Логирование и мониторинг активности пользователей»	*2*	
	В том числе, самостоятельных работ:	***2***	
	Самостоятельная работа №1 «Анализ веб-приложения на предмет угроз безопасности»	*2*	
	Раздел 2. Борьба с вирусным заражением	***46***	
Тема 2.1. Проблема вирусного заражения и структура современных вирусов	**Содержание учебного материала**	***22***	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 5.6
	1. Общая характеристика компьютерных вирусов. Классификация компьютерных вирусов. Признаки проявления вирусов. Структура вирусов, пути их распространения. Кейлоггеры. Классификация по типу, по месту хранения, по методу отправки и методу применения. 2. Модели поведения вирусов и их деструктивные действия		
	В том числе, практических занятий:	***8***	
	Практическое занятие №8 «Анализ веб-сценариев на наличие вредоносного кода»	*2*	
	Практическое занятие №9 «Проверка веб-скриптов на наличие подозрительного кода»	*2*	
	Практическое занятие №10 «Реализация базовых мер защиты веб-приложений от вредоносного кода»	*2*	
	Практическое занятие №11 «Проверка веб-скриптов на вирусы и вредоносные элементы»	*2*	
	В том числе, самостоятельных работ:	***2***	
	Самостоятельная работа №2 «Создание руководства по защите веб-приложений от вредоносного кода»	*2*	
Тема 2.2. Защита от воздействия вирусов	**Содержание учебного материала**	***24***	ОК 01, ОК 02, ОК 05, ОК 09, ПК 5.3, ПК 5.6
	Классификация методов защиты от компьютерных вирусов. Виды и назначение антивирусных программ. Состав программного комплекса защиты от вирусов. Общая характеристика средств нейтрализации компьютерных вирусов.		
	В том числе, практических занятий:	***8***	
	Практическое занятие №12 «Настройка прав доступа и фильтров в веб-приложении на PHP»	*2*	
	Практическое занятие №13 «Средства аутентификации и авторизации»	*2*	

	Практическое занятие №14 «Защита пользовательских данных в учебной БД и проверка ограничений доступа»	*2*	
	Практическое занятие №15 «Создание резервных копий и восстановление данных после имитации заражения»	*2*	
	В том числе, самостоятельных работ:	***4***	
	Самостоятельная работа №3 «Анализ веб-сервера на уязвимости и риски заражения»	*2*	
	Самостоятельная работа №4 «Разработка мер защиты веб-приложения от SQL-инъекций, XSS и других целевых атак»	*2*	
	Консультации перед экзаменом	***4***	
	Промежуточная аттестация в форме экзамена	***6***	
	Всего	**88**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы дисциплины должны быть предусмотрены следующие специальные помещения

Реализация программы дисциплины требует наличия учебного кабинета системного и прикладного программирования.

Помещение кабинета должно соответствовать действующим санитарно-эпидемиологическим требованиям, быть оснащено специализированной учебной мебелью и средствами обучения, необходимыми для выполнения требований к уровню подготовки обучающихся.

Оборудование учебного кабинета:

– посадочные места по количеству обучающихся;

– автоматизированное рабочее место преподавателя;

– наглядные пособия и демонстрационные материалы;

– профессионально ориентированные задания;

– материалы для текущего контроля и промежуточной аттестации.

Технические средства обучения и программное обеспечение:

— мультимедиапроектор;

— персональные компьютеры с операционной системой Windows;

— доступ к сети Интернет;

— программное обеспечение для выполнения практических работ: VirtualBox, PyCharm Professional, XAMPP, OpenServer, браузеры, антивирусное программное обеспечение, средства резервного копирования;

— средства просмотра и анализа журналов событий, логов веб-сервера и активности пользователей.

3.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

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

Перечень основных печатных и/или электронных изданий, а также дополнительных источников приведён в разделе 4 настоящей рабочей программы.

4. ПЕЧАТНЫЕ И ЭЛЕКТРОННЫЕ ИЗДАНИЯ

4.1. Основные печатные и/или электронные издания

1. Козырь, Н. С., Оганесян, Л. Л. Экономические аспекты информационной безопасности: учебник и практикум для вузов. — Москва: Издательство Юрайт, 2025. — 131 с. — ISBN 978-5-534-17863-0. — URL: https://urait.ru/bcode/568708
2. Чернова, Е. В. Информационная безопасность человека: учебник для вузов. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 327 с. — ISBN 978-5-534-16772-6. — URL: https://urait.ru/bcode/566457
3. Козырь, Н. С., Седых, Н. В. Гуманитарные аспекты информационной безопасности: учебник для вузов. — Москва: Издательство Юрайт, 2025. — 170 с. — ISBN 978-5-534-17153-2. — URL: https://urait.ru/bcode/568566
4. Суворова, Г. М. Информационная безопасность: учебник для вузов. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 277 с. — ISBN 978-5-534-16450-3. — URL: https://urait.ru/bcode/567672
5. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 107 с. — ISBN 978-5-534-16388-9. — URL: https://urait.ru/bcode/567915

4.2. Дополнительные электронные ресурсы

1. Официальный сайт ФСТЭК России — https://fstec.ru/
2. Официальный сайт Роскомнадзора — https://rkn.gov.ru/
3. OWASP Web Security Testing Guide — https://owasp.org/www-project-web-security-testing-guide/
4. OWASP Top 10 — https://owasp.org/www-project-top-ten/
5. Microsoft Learn: Security documentation — https://learn.microsoft.com/security/
6. Национальный открытый университет «ИНТУИТ» — https://intuit.ru/studies/courses/28/28/info

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляются преподавателем в процессе проведения текущего контроля, выполнения практических занятий, самостоятельных работ, индивидуальных заданий, а также промежуточной аттестации в форме экзамена.

Код ОК/ПК	Результаты обучения	Критерии оценки	Формы и методы оценки
ОК 01	Определять уровень угроз информационной безопасности; оценивать риски для информационных систем.	Обучающийся распознаёт задачу в области информационной безопасности, определяет возможные угрозы и риски, выбирает способы их устранения или снижения, обосновывает выбранные меры защиты.	Устный и письменный опрос; компьютерное тестирование; выполнение практических работ; решение ситуационных задач; оценка выполнения самостоятельной работы.
ОК 02	Проводить сбор и анализ информации о потенциальных угрозах; оценивать защитные меры.	Обучающийся использует нормативные, справочные и электронные источники информации, анализирует сведения об угрозах информационной безопасности, выделяет значимую информацию и применяет её при решении практических задач.	Практические работы; анализ кейсов; подготовка отчётов; самостоятельная работа; тестирование по темам дисциплины.
ОК 05	Разрабатывать и оформлять отчёты и инструкции по информационной безопасности; составлять рекомендации.	Обучающийся грамотно оформляет результаты выполнения практических заданий, составляет инструкции, отчёты и рекомендации по обеспечению информационной безопасности с учётом профессиональной терминологии.	Проверка отчётов по практическим работам; оценка индивидуальных заданий; защита выполненных работ; письменный опрос.
ОК 09	Использовать ИТ-средства для реализации мер информационной безопасности.	Обучающийся применяет программные средства и цифровые инструменты для настройки защиты данных, аутентификации, разграничения доступа, резервного копирования, анализа угроз и мониторинга безопасности.	Наблюдение за выполнением практических заданий; оценка практических работ; компьютерное тестирование; экзамен.
ПК 5.3	Разрабатывать и применять базовые меры защиты информационных систем.	Обучающийся определяет угрозы информационной безопасности, подбирает и применяет средства защиты, выполняет настройку аутентификации, разграничения доступа, логирования, резервного копирования и защиты веб-приложений от типовых атак.	Выполнение практических работ; решение ситуационных задач; защита отчётов; оценка практического задания на экзамене.

ПК 5.6	Подготавливать документацию по обеспечению информационной безопасности.	Обучающийся оформляет техническую и эксплуатационную документацию по обеспечению информационной безопасности, разрабатывает инструкции и рекомендации по защите информационных систем и пользовательских данных.	Проверка отчётов и инструкций; оценка самостоятельных работ; защита индивидуального задания; экзамен.

Обобщённые критерии оценки результатов освоения дисциплины

1. Оценка **«отлично»** выставляется, если обучающийся полностью освоил теоретическое содержание дисциплины, правильно применяет понятия и методы информационной безопасности, самостоятельно выполняет практические задания, обоснованно выбирает меры защиты информации, грамотно оформляет результаты работы.

2. Оценка **«хорошо»** выставляется, если обучающийся освоил основное содержание дисциплины, выполняет практические задания с незначительными ошибками, умеет применять средства защиты информации и оформлять результаты работы, но отдельные решения требуют уточнения или доработки.

3. Оценка **«удовлетворительно»** выставляется, если обучающийся освоил содержание дисциплины частично, допускает ошибки при анализе угроз и выборе мер защиты, выполняет практические задания с помощью преподавателя или по образцу, оформление результатов содержит недочёты.

4. Оценка **«неудовлетворительно»** выставляется, если обучающийся не освоил основное содержание дисциплины, не умеет определять угрозы информационной безопасности, не выполняет практические задания или допускает грубые ошибки при выборе и применении мер защиты информации