Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ганеев Винер Валиахметович
Должность: Директор
Дата подписания: 17.11.2026 13:13:34
Уникальный программный ключ:
fceab25d7092f3bff743e8ad3f8d57fddc1f5e66

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Уфимский университет науки и технологий»
Бирский филиал
Колледж

ОДОБРЕНО
на заседании ПЦК технических и прикладных дисциплин
протокол №01 от «30» августа 2026 г.
Председатель ПЦК
_____ А.Ю.Воробьев

УТВЕРЖДАЮ

Заведующий колледжем
_____ А.А. Русинов
«30» августа 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.09 Основы защиты информации

шифр и наименование
09.02.01 Компьютерные системы и комплексы

Квалификация выпускника

специалист по компьютерным системам

Форма обучения: очная

Бирск – 2026

Рабочая программа разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности **09.02.01 Компьютерные системы и комплексы**, утвержденного приказом Минпросвещения России от 25 мая 2022 г. № 362 (в ред. от 03.07.2024).

Организация-разработчик: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский университет науки и технологий», **Бирский филиал, колледж**.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
   1.1. Область применения рабочей программы
   1.2. Место учебной дисциплины в структуре образовательной программы
   1.3. Цель и планируемые результаты освоения дисциплины
2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
   2.1. Объем дисциплины и виды учебной работы
   2.2. Тематический план и содержание дисциплины
3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ
4. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ
   4.1. Требования к минимальному материально-техническому обеспечению
   4.2. Учебно-методическое и информационное обеспечение дисциплины
5. ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

ПРИЛОЖЕНИЕ 1

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа дисциплины является частью образовательной программы в соответствии с ФГОС СПО по специальности:

09.02.01 Компьютерные системы и комплексы

(укрупнённая группа специальностей **09.00.00 Информатика и вычислительная техника**),

для обучающихся **очной** формы обучения.

1.2. Место учебной дисциплины в структуре образовательной программы

Дисциплина **ОП.09 Основы защиты информации** относится к **общепрофессиональному циклу** образовательной программы.

Дисциплина реализуется в рамках **обязательной** части.

Дисциплина изучается на **4 курсе** в **1 семестре**.

1.3. Цель и планируемые результаты освоения дисциплины

Цель дисциплины: формирование у обучающихся системы знаний и умений в области защиты информации, обеспечение безопасного функционирования компьютерных систем и комплексов, а также формирование навыков применения программно-аппаратных средств защиты информации.

Задачи дисциплины:

- изучение основных понятий, принципов и методов защиты информации;
- освоение нормативно-правовой базы в области информационной безопасности;
- формирование навыков выявления угроз безопасности информации и каналов утечки;
- изучение программно-аппаратных средств защиты информации;
- развитие умений применять средства защиты информации в профессиональной деятельности;

- формирование навыков организации защиты информации в компьютерных системах.

Планируемые результаты освоения дисциплины:

Код ОК	Умения	Знания
ОК 01	Распознавать задачу и/или проблему в профессиональном и/или социальном контексте; определять этапы решения задачи; выявлять и эффективно искать информацию	Актуальный профессиональный и социальный контекст; основные источники информации и ресурсы для решения задач
ОК 02	Определять задачи для поиска информации; планировать процесс поиска; структурировать получаемую информацию	Номенклатура информационных источников; приемы структурирования информации
ОК 03	Определять актуальность нормативно-правовой документации; применять современную научную профессиональную терминологию	Содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология
ОК 04	Организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами	Психологические основы деятельности коллектива
ОК 05	Грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке	Особенности социального и культурного контекста; правила оформления документов
ОК 06	Проявлять гражданско-патриотическую позицию; демонстрировать осознанное поведение	Сущность гражданско-патриотической позиции; общечеловеческие ценности
ОК 07	Соблюдать нормы экологической безопасности; определять направления ресурсосбережения	Правила экологической безопасности; принципы бережливого производства
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья	Роль физической культуры в общекультурном и профессиональном развитии

Код ОК	Умения	Знания
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	Правила построения простых и сложных предложений на профессиональные темы

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Очная форма обучения

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**112**
Обязательная аудиторная учебная нагрузка (всего)	**92**
в том числе:	
лекции (уроки)	52
практические занятия	40
лабораторные занятия	—
курсовая работа (проект) (если предусмотрена)	—
Самостоятельная работа обучающегося (всего)	**20**
- индивидуальный проект (если предусмотрен)	—
Промежуточная аттестация в форме **дифференцированного зачета** в **1** семестре	

Распределение по семестрам:

Курс	Семестр	Объем часов	Вид промежуточной аттестации
4 курс	**1 семестр**	**112**	**дифференцированный зачет**
Итого		**112**	

2.2. Тематический план и содержание дисциплины

Очная форма обучения

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
1	**2**	**3**	**4**

Наименование разделов и тем	**Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся**	**Объем часов**	**Формируемые компетенции**
Раздел 1. Основы защиты информации		**32**	
Тема 1.1. Введение. Основные понятия и определения	Содержание учебного материала:	4	ОК 01, ОК 02
	1. Понятие информации, информационной безопасности, защиты информации.		
	2. Основные свойства информации: конфиденциальность, целостность, доступность.		
	3. Роль и место защиты информации в современном обществе.		
	Практические занятия:	2	
	1. Анализ основных понятий и определений.		
	Самостоятельная работа:	2	
	1. Подготовка сообщения «История развития защиты информации».		
Тема 1.2. Нормативно-правовая база защиты информации	Содержание учебного материала:	6	ОК 01, ОК 03, ОК 05
	1. Федеральные законы в области защиты информации.		
	2. Доктрина информационной безопасности Российской Федерации.		

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
	3. Стандарты и нормативные документы в области защиты информации.		
	Практические занятия:	4	
	1. Анализ Федерального закона «Об информации, информационных технологиях и о защите информации».		
	2. Изучение Доктрины информационной безопасности.		
	Самостоятельная работа:	2	
	1. Составление таблицы «Основные нормативные документы в области защиты информации».		
Тема 1.3. Угрозы безопасности информации	Содержание учебного материала:	6	ОК 01, ОК 02
	1. Классификация угроз безопасности информации.		
	2. Каналы утечки информации.		
	3. Методы выявления угроз.		
	Практические занятия:	4	
	1. Анализ типовых угроз безопасности информации.		
	2. Выявление каналов утечки информации.		
	Самостоятельная работа:	2	

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
	1. Составление схемы каналов утечки информации.		
Тема 1.4. Методы и средства защиты информации	Содержание учебного материала:	8	ОК 01, ОК 02, ОК 03
	1. Правовые методы защиты информации.		
	2. Организационные методы защиты информации.		
	3. Инженерно-технические методы защиты информации.		
	4. Программно-аппаратные средства защиты информации.		
	Практические занятия:	4	
	1. Классификация методов и средств защиты информации.		
	2. Изучение программно-аппаратных средств защиты.		
	Самостоятельная работа:	2	
	1. Составление сравнительной таблицы методов защиты информации.		
Тема 1.5. Криптографические методы защиты информации	Содержание учебного материала:	8	ОК 01, ОК 02, ОК 03
	1. Основные понятия криптографии.		

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
	2. Симметричные и асимметричные алгоритмы шифрования.		
	3. Электронная цифровая подпись.		
	Практические занятия:	4	
	1. Изучение симметричных алгоритмов шифрования.		
	2. Изучение асимметричных алгоритмов шифрования.		
	3. Работа с электронной цифровой подписью.		
	Самостоятельная работа:	2	
	1. Изучение алгоритма RSA.		
Раздел 2. Защита информации в компьютерных системах		**40**	
Тема 2.1. Защита информации в операционных системах	Содержание учебного материала:	8	ОК 01, ОК 02
	1. Идентификация и аутентификация пользователей.		
	2. Управление доступом в операционных системах.		
	3. Аудит и регистрация событий безопасности.		
	Практические занятия:	6	
	1. Настройка идентификации и аутентификации в ОС.		

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
	2. Настройка управления доступом.		
	3. Анализ журналов событий безопасности.		
	Самостоятельная работа:	2	
	1. Изучение моделей управления доступом.		
Тема 2.2. Антивирусная защита	Содержание учебного материала:	6	ОК 01, ОК 02
	1. Классификация вредоносных программ.		
	2. Методы обнаружения вредоносных программ.		
	3. Антивирусные программы и их настройка.		
	Практические занятия:	4	
	1. Установка и настройка антивирусной программы.		
	2. Проверка системы на наличие вредоносных программ.		
	Самостоятельная работа:	2	
	1. Изучение методов обнаружения вредоносных программ.		
Тема 2.3. Сетевая защита информации	Содержание учебного материала:	8	ОК 01, ОК 02, ОК 04
	1. Межсетевые экраны (firewall).		
	2. Защита беспроводных сетей.		
	3. Виртуальные частные сети (VPN).		
	Практические занятия:	4	

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
	1. Настройка межсетевого экрана.		
	2. Настройка защиты беспроводной сети.		
	3. Настройка VPN-соединения.		
	Самостоятельная работа:	2	
	1. Изучение принципов работы VPN.		
Тема 2.4. Защита информации в базах данных	Содержание учебного материала:	6	ОК 01, ОК 02
	1. Угрозы безопасности баз данных.		
	2. Методы защиты баз данных.		
	3. Резервное копирование и восстановление данных.		
	Практические занятия:	4	
	1. Настройка защиты базы данных.		
	2. Выполнение резервного копирования и восстановления.		
	Самостоятельная работа:	2	
	1. Изучение методов защиты баз данных.		
Тема 2.5. Организация защиты информации на предприятии	Содержание учебного материала:	6	ОК 01, ОК 02, ОК 04, ОК 06
	1. Политика информационной безопасности.		

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
	2. Организационные меры защиты информации.		
	3. Обучение персонала в области информационной безопасности.		
	Практические занятия:	2	
	1. Разработка политики информационной безопасности.		
	Самостоятельная работа:	2	
	1. Разработка инструкции по информационной безопасности для персонала.		
Раздел 3. Применение средств защиты информации		**36**	
Тема 3.1. Программно-аппаратные средства защиты информации	Содержание учебного материала:	8	ОК 01, ОК 02
	1. Средства защиты от несанкционированного доступа.		
	2. Системы обнаружения вторжений.		
	3. Средства криптографической защиты информации.		
	Практические занятия:	6	
	1. Настройка средств защиты от несанкционированного доступа.		

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
	2. Изучение работы системы обнаружения вторжений.		
	Самостоятельная работа:	2	
	1. Изучение классификации программно-аппаратных средств защиты.		
Тема 3.2. Защита информации при работе в сети Интернет	Содержание учебного материала:	6	ОК 01, ОК 02, ОК 05
	1. Безопасность при работе в сети Интернет.		
	2. Защита персональных данных.		
	3. Безопасное использование облачных сервисов.		
	Практические занятия:	4	
	1. Настройка безопасного подключения к сети Интернет.		
	2. Анализ рисков при работе с облачными сервисами.		
	Самостоятельная работа:	2	
	1. Изучение методов защиты персональных данных.		
Тема 3.3. Аудит и оценка эффективности системы защиты информации	Содержание учебного материала:	6	ОК 01, ОК 02, ОК 03

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
	1. Методы аудита информационной безопасности.		
	2. Оценка эффективности системы защиты информации.		
	3. Документирование результатов аудита.		
	Практические занятия:	4	
	1. Проведение аудита системы защиты информации.		
	2. Оформление отчета по результатам аудита.		
	Самостоятельная работа:	2	
	1. Изучение методов оценки эффективности защиты информации.		
Промежуточная аттестация		**4**	
Всего:		**112**	

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств (ФОС) — комплект методических и контрольных материалов, используемых при проведении текущего контроля освоения результатов обучения и промежуточной аттестации. ФОС предназначен для контроля и управления процессом приобретения обучающимися необходимых знаний, умений и компетенций, определённых во ФГОС СПО.

Типовые контрольные оценочные средства представлены в Приложении 1.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета **«Основы защиты информации»**.

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий (плакаты, схемы, таблицы);
- персональные компьютеры с лицензионным программным обеспечением;
- мультимедийный проектор;
- интерактивная доска (при наличии).

4.2. Учебно-методическое и информационное обеспечение дисциплины

4.2.1. Перечень основной и дополнительной учебной литературы

Основная учебная литература:

1. Мельников, В. П. Информационная безопасность : учебник для среднего профессионального образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков. — 8-е изд., стер. — Москва : Академия, 2022. — 336 с. — ISBN 978-5-0053-0321-6.
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 416 с. — ISBN 978-5-8199-0765-6.
3. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — Москва : ИНТУИТ, 2021. — 264 с.

Дополнительная учебная литература:

1. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с.
2. Бабаш, А. В. Информационная безопасность : практикум / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КНОРУС, 2022. — 256 с.
3. Конеев, И. Р. Информационная безопасность предприятия : учебное пособие / И. Р. Конеев, А. В. Беляев. — Санкт-Петербург : БХВ-Петербург, 2020. — 752 с.

4.2.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

№	Наименование электронной библиотечной системы
1.	ЭБС «Лань» — https://e.lanbook.com
2.	Образовательная платформа «Юрайт» — https://urait.ru
3.	Электронный ресурс цифровой образовательной среды СПО PROFобразование — https://profspo.ru
№	**Адрес (URL)**
1.	https://fstec.ru — Федеральная служба по техническому и экспортному контролю
2.	https://www.consultant.ru — Справочно-правовая система «КонсультантПлюс»
3.	https://www.garant.ru — Информационно-правовой портал «Гарант»

4.2.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса

Наименование программного обеспечения

Microsoft Windows

Microsoft Office

LibreOffice

Антивирусные программы (Kaspersky, Dr.Web)

Межсетевые экраны (Windows Firewall, Comodo)

Справочно-правовая система «КонсультантПлюс»

5. ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

5.1. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

Активные и интерактивные формы проведения занятий:

- групповые дискуссии по проблемным вопросам защиты информации;
- разбор конкретных ситуаций (инциденты информационной безопасности);
- работа в малых группах при выполнении практических работ;
- деловые и ролевые игры (моделирование ситуаций нарушения безопасности);
- круглые столы по актуальным проблемам информационной безопасности;
- компьютерные симуляции (моделирование атак и защиты).

ПРИЛОЖЕНИЕ 1

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский университет науки и технологий»
Бирский филиал
колледж

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
ОП.09 Основы защиты информации

шифр наименование
Наименование специальности: **09.02.01 Компьютерные системы и комплексы**

Квалификация выпускника: **специалист по компьютерным системам**

Форма обучения: **очная**

Бирск — 2026

Фонд оценочных средств по дисциплине **ОП.09 Основы защиты информации** разработан на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности **09.02.01 Компьютерные системы и комплексы**, утвержденного приказом Минпросвещения России от 25 мая 2022 г. № 362 (в ред. от 03.07.2024), и рабочей программы дисциплины.

1. Область применения

Фонд оценочных средств (ФОС) предназначен для контроля и оценки результатов освоения дисциплины **ОП.09 Основы защиты информации**, образовательной программы по специальности СПО **09.02.01 Компьютерные системы и комплексы**.

2. Объекты оценивания — результаты освоения

В результате промежуточной аттестации по дисциплине осуществляется комплексная оценка овладения следующими знаниями и умениями:

Знания:

- основных понятий и определений в области защиты информации;
- нормативно-правовой базы защиты информации;
- классификации угроз безопасности информации;
- каналов утечки информации;
- методов и средств защиты информации;
- криптографических методов защиты информации;
- принципов защиты информации в операционных системах, базах данных, сетях;
- программно-аппаратных средств защиты информации.

Умения:

- выявлять угрозы безопасности информации;
- определять каналы утечки информации;
- применять методы и средства защиты информации;
- настраивать средства защиты информации в операционных системах;

- использовать антивирусные программы и межсетевые экраны;
- выполнять резервное копирование и восстановление данных;
- разрабатывать политику информационной безопасности;
- проводить аудит системы защиты информации.

3. Формы контроля и оценки результатов освоения дисциплины

3.1. Формы текущего контроля

- устный опрос;
- тестирование;
- проверка выполнения практических заданий;
- проверка лабораторных работ;
- защита отчетов по практическим работам;
- контроль самостоятельной работы.

3.2. Форма промежуточной аттестации

Промежуточная аттестация по дисциплине — **дифференцированный зачет** (1 семестр 4 курса).

Обучающиеся допускаются к сдаче дифференцированного зачета при условии выполнения всех видов работ, предусмотренных рабочей программой.

4. Типовые контрольные задания для дифференцированного зачета

Перечень вопросов к дифференцированному зачету:

1. Понятие информации, информационной безопасности, защиты информации.
2. Основные свойства информации: конфиденциальность, целостность, доступность.
3. Федеральные законы в области защиты информации.
4. Доктрина информационной безопасности Российской Федерации.
5. Классификация угроз безопасности информации.
6. Каналы утечки информации.
7. Правовые методы защиты информации.
8. Организационные методы защиты информации.
9. Инженерно-технические методы защиты информации.

10. Программно-аппаратные средства защиты информации.
11. Основные понятия криптографии.
12. Симметричные алгоритмы шифрования.
13. Асимметричные алгоритмы шифрования.
14. Электронная цифровая подпись.
15. Идентификация и аутентификация пользователей.
16. Управление доступом в операционных системах.
17. Аудит и регистрация событий безопасности.
18. Классификация вредоносных программ.
19. Методы обнаружения вредоносных программ.
20. Антивирусные программы и их настройка.
21. Межсетевые экраны (firewall).
22. Защита беспроводных сетей.
23. Виртуальные частные сети (VPN).
24. Угрозы безопасности баз данных.
25. Методы защиты баз данных.
26. Резервное копирование и восстановление данных.
27. Политика информационной безопасности.
28. Организационные меры защиты информации.
29. Средства защиты от несанкционированного доступа.
30. Системы обнаружения вторжений.
31. Безопасность при работе в сети Интернет.
32. Защита персональных данных.
33. Методы аудита информационной безопасности.
34. Оценка эффективности системы защиты информации.

Тестовые задания (пример):

1. Какое свойство информации означает её защиту от несанкционированного изменения?
    - а) конфиденциальность;
    - б) целостность;

- в) доступность;
- г) достоверность.

2. Какой документ определяет государственную политику в области информационной безопасности?
   - а) Федеральный закон «Об информации»;
   - б) Доктрина информационной безопасности;
   - в) Конституция РФ;
   - г) Уголовный кодекс РФ.
3. Какой метод защиты информации основан на преобразовании информации с целью её сокрытия?
   - а) организационный;
   - б) криптографический;
   - в) правовой;
   - г) инженерно-технический.
4. Что такое электронная цифровая подпись?
   - а) реквизит электронного документа;
   - б) программа для шифрования;
   - в) антивирусная программа;
   - г) межсетевой экран.
5. Какое средство защиты используется для фильтрации сетевого трафика?
   - а) антивирус;
   - б) межсетевой экран;
   - в) криптографическая программа;
   - г) система обнаружения вторжений.