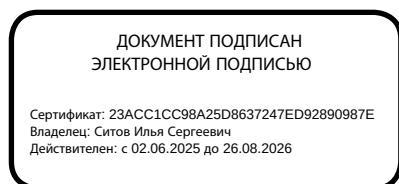


Министерство науки и высшего образования Российской Федерации
Многопрофильный колледж
федерального государственного бюджетного образовательного учреждения
высшего образования
«Братский государственный университет»



УТВЕРЖДАЮ
Председатель научно-методического совета
_____ А.В. Долгих
« ____ » _____ 2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для специальности среднего профессионального образования
09.02.11 Разработка и управление программным обеспечением
«Общепрофессиональный цикл»

2026 г.

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, входящей в укрупненную группу специальностей 09.00.00 Информатика и вычислительная техника.

Организация-разработчик: Многопрофильный колледж ФГБОУ ВО «БрГУ»

Разработчик:

Ратинская Екатерина Валерьевна, преподаватель.

Рабочая программа рекомендована дисциплинарно-цикловой комиссией дисциплин предметной подготовки.

от «22» мая 2026 г., протокол №3

Рабочая программа одобрена научно-методическим советом

от «29» мая 2026 г., протокол №3

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	стр. 4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	10
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	12

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности среднего профессионального образования (далее СПО) 09.02.11 Разработка и управление программным обеспечением, входящей в укрупненную группу специальностей 09.00.00 Информатика и вычислительная техника.

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

дисциплина входит в общепрофессиональный цикл.

1.3. Цели и задачи учебной дисциплины - требования к результатам освоения учебной дисциплины:

Цель: 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.

В результате освоения учебной дисциплины обучающийся должен владеть навыками:

- применение современных методов и технологий в области безопасности информационных систем.

В результате освоения учебной дисциплины обучающийся должен уметь:

- 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 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;
- понимать тексты на базовые профессиональные темы;
- шифровать данные и обеспечивать их конфиденциальность;
- анализ требований безопасности информационных систем.

В результате освоения учебной дисциплины обучающийся должен знать:

- 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;
- 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.
- 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.;
- отраслевая нормативная техническая документация;
- источники информации, необходимой для профессиональной деятельности;
- современный отечественный и зарубежный опыт в профессиональной деятельности;
- принципы и методы обеспечения 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.

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

максимальной учебной нагрузки обучающегося **34** часа, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося **34** часа;
- самостоятельной работы обучающегося **0** часов.
- консультации **0** часов;
- промежуточная аттестация **0** часов.

1.5. Формируемые компетенции

Изучение учебной дисциплины направлено на формирование следующих компетенций:

ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 2. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной

деятельности.

ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 1.1. Проектировать базы данных.

ПК 1.4. Администрировать базы данных.

ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации.

ПК 3.1. Собирать исходные данные для разработки проектной документации на информационную систему.

ПК 3.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	<i>Объем часов</i>
Максимальная учебная нагрузка (всего)	34
Обязательная аудиторная учебная нагрузка (всего)	34
в том числе:	
теоретические занятия	17
практические занятия	0
лабораторные занятия	17
Самостоятельная работа обучающегося (всего)	0
в том числе:	
внеаудиторная самостоятельная работа	0
Итоговая аттестация в форме <i>дифференцированного зачета</i>	

2.2. Календарно-тематический план и содержание учебной дисциплины АРХИТЕКТУРА АППАРАТНЫХ СРЕДСТВ

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Учебная неделя	Уровень усвоения	Формируемые компетенции
1	2	3		4	5
Тема 1.1. Введение в информационную безопасность	Содержание учебного материала Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	1	1	1, 2	ОК 1 ОК 2 ОК 9 ПК 1.1. ПК 1.4. ПК 1.5. ПК 3.1. ПК 3.3.
Тема 1.2. Управление безопасностью информации	Содержание учебного материала Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2	2,3	1,2	
Тема 1.3. Криптография	Содержание учебного материала Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	4,5	2,3	
	Лабораторные занятия: 1. Работа с симметричными и асимметричными алгоритмами. 2. Хэширование и создание цифровой подписи сообщения.	2	<u>1,2</u>	3	
Тема 1.4. Защита сетевой инфраструктуры	Содержание учебного материала Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	2	6,7	1,2	
	Лабораторные занятия: 1. Организация защиты от атак. 2. Организация работы VPN и межсетевого экрана.	4	<u>3-6</u>	3	
Тема 1.5. Безопасность приложений	Содержание учебного материала Уязвимости веб-приложений (OWASP TopTen). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	8,9	2,3	
	Лабораторные занятия: 1. Тестирование на проникновение и анализ уязвимостей.	2	<u>7,8</u>	3	
Тема 1.6. Защита данных	Содержание учебного материала Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным.	2	10,11	1,2	
	Лабораторные занятия: 1. Выполнение резервного копирования и восстановления данных. 2. Управление доступом к данным	4	<u>9-12</u>	3	
Тема 1.7. Безопасность облачных технологий	Содержание учебного материала Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности.	1	12	2,3	
	Лабораторные занятия: 1. Изучение модели облачных услуг и их безопасности.	2	<u>13,14</u>	3	
Тема 1.8. Инциденты безопасности	Содержание учебного материала Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT.	2	13,14	2,3	

	Форензика.				
	Лабораторные занятия: 1. Работа с инцидентами.	2	<u>15,16</u>	3	
Тема 1.9. Социальная инженерия и человеческий фактор	Содержание учебного материала				
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности..	1	15	2,3	
	Лабораторные занятия: 1. Разработка политики информационной безопасности.	1	<u>17</u>	3	
Тема 1.10. Будущее информационной безопасности	Содержание учебного материала				
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности.	1	16	2	
Дифференцированный зачет		1	17		
Всего:		34			

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

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия лаборатории Вычислительной техники, архитектуры персонального компьютера и периферийных устройств.

Оборудование лаборатории Вычислительной техники, архитектуры персонального компьютера и периферийных устройств:

- Автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;) или аналоги;
- Автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;) или аналоги;
- 12-15 комплектов компьютерных комплектующих для производства сборки, разборки и сервисного обслуживания ПК и оргтехники;
- Специализированная мебель для сервисного обслуживания ПК с заземлением и защитой от статического напряжения;
- Проектор и экран;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, дополнительной литературы, Интернет-ресурсов.

Основная литература:

1. Гриценко Ю.Б. Вычислительные системы, сети и телекоммуникации: учебное пособие / Ю.Б. Гриценко; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР), Факультет дистанционного обучения. - Томск: ТУСУР, 2025. - 134с.: схем., табл., ил. - Библиогр.: с. 123-124; [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=480639>.
2. Куль Т.П. Основы вычислительной техники: учебное пособие / Т.П. Куль. - Минск: РИПО, 2024. - 244 с.: ил., табл., схем. - Библиогр.: с. 257-258 - ISBN 978-985-503-812-3; [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=497477>.
3. Рыбальченко М.В. Архитектура информационных систем: учебное пособие / М.В. Рыбальченко; Министерство образования и науки Российской Федерации, Южный федеральный университет. - Таганрог: Издательство Южного федерального университета, 2055. - Ч. 1. - 92 с. - Библиогр. в кн. - ISBN 978-5-9275-1765-7; [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=462011>.

Дополнительная литература:

1. Богомолов С.А. Основы электроники и цифровой схемотехники. - М.: Академия, 2023. -208с.
2. Бубнов А.А. Основы информационной. - М.: Академия, 2025. -256с.
3. Колдаев В.Д. Архитектура ЭВМ. - М.: ИНФРА-М, 20246. 384 с.
4. Поршнева С.В. Сборник олимпиадных задач для специальности Вычислительные машины, комплексы, системы и сети. – М.: Кно-Рус, 2026. - 280с.
5. Струмпэ Н.В. Аппаратное обеспечение ЭВМ. Практикум. - М.: Академия, 2025. - 160с.

6. Черников Б.В. Управление качеством программного обеспечения. Учебник - М.: ФОРУМ: ИИНФРА-М, 2025. -240с.

Интернет – ресурсы:

1. Википедия – Свободная энциклопедия. Режим доступа: [<http://ru.wikipedia.org>] (дата обращения 21.05.2026).
2. Нетбуки. Планшеты. Сенсорные телефоны. Мобильные компьютеры. Гаджеты. Обзоры устройств. Технологии. Режим доступа: [<http://hi-tech.mail.ru>] (дата обращения 21.05.2026).
3. Оперативные новости, обзоры и тестирования компьютеров, видеокарт, процессоров, материнских плат, памяти и принтеров, цифровых фотоаппаратов и видеокамер, смартфонов и планшетов, мониторов и проекторов. Режим доступа: [<http://www.ixbt.com>] (дата обращения 21.05.2026).
4. Матбюро: учебники по теории вероятностей. Режим доступа [http://www.matburo.ru/st_subject.php?p=tv] (дата обращения 21.05.2026).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
Владеть навыками: – применение современных методов и технологий в области безопасности информационных систем. Уметь: – 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 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; – понимать тексты на базовые профессиональные темы; – шифровать данные и обеспечивать их конфиденциальность; – анализ требований безопасности информационных систем. Знать:	Текущий контроль: - устный опрос по теоретическому материалу; - письменные самостоятельные работы; - проверка выполнения домашних заданий; - защита рефератов; - оценка защиты лабораторных работ; - доклады, подготовленные в процессе самостоятельной работы. Промежуточная аттестация в форме дифференцированного зачета

– 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; – 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. – 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.; – отраслевая нормативная техническая документация; – источники информации, необходимой для профессиональной деятельности; – современный отечественный и зарубежный опыт в профессиональной деятельности; – принципы и методы обеспечения 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.	
---	--