МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«АРКТИЧЕСКИЙ ГОСУДАРСТВЕННЫЙ АГРОТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО Арктический ГАТУ)
Колледж технологий и управления

Регистрационный
№ 24-01/24

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина **ОП.05 Основы информационной безопасности**

Специальность **09.02.11 Разработка и управление программным обеспечением**

Квалификация **Программист**

Уровень ППССЗ **базовая**

Срок освоения ППССЗ **3 г 10 мес**

Форма обучения **очная**

Общая трудоемкость **72 ч**

Якутск 2026

Рабочая программа учебной дисциплины разработана в соответствии с:
- Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением, утвержденным приказом Министерства образования и науки Российской Федерации от 24.02.2025 № 138.
- Учебным планом специальности 09.02.11 Разработка и управление программным обеспечением одобренным Ученым советом ФГБОУ ВО Арктический ГАТУ от 02.04.2026 г. № 56.

Разработчик(и) РПД Федоров Павел Иванович – преподаватель

Председатель цикловой комиссии ГиЕД _____/Васильева Е.К./
подпись фамилия, имя, отчество

Протокол заседания цикловой комиссии ГиЕД №10 от «13» марта 2026 г

Директор КТиУ _____/Яковлева Н.М./
подпись фамилия, имя, отчество

«20» марта 2026 г.

Председатель МК КТиУ _____ /Ваганова В.Г./
подпись фамилия, имя, отчество

Протокол заседания МК КТиУ № 3 от «20» марта 2026 г

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
09.02.11 Разработка и управление программным обеспечением

1.1. Область применения программы. Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.11 Разработка и управление программным обеспечением.
1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена. Учебная **дисциплина «ОП.05 Основы информационной безопасности» относится к общепрофессиональному** циклу.
Освоение дисциплины способствует формированию компетенций:

- ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
- ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
- ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.
- ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
- ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины

Цель дисциплины: 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.

Задача дисциплины: обеспечить обучающихся теоретическими знаниями и практическими навыками в области обеспечения информационной безопасности, необходимыми для разработки и эксплуатации защищенных программных систем.

В результате освоения учебной дисциплины обучающийся должен уметь:

- У.1. 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.
- У.2. 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.
- У.3. Оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач.
- У.4. Понимать тексты на базовые профессиональные темы (на иностранном языке).
- У.5. Шифровать данные и обеспечивать их конфиденциальность.

В результате освоения учебной дисциплины обучающийся должен знать:

- З.1. 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.
- З.2. Номенклатуру информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации.
- З.3. Основные принципы и методы обеспечения безопасности информационных систем.
- З.4. Принципы криптографии и методов шифрования данных; стандарты и протоколы безопасности (SSL/TLS, SSH, Kerberos, HTTPS, OAuth и др.).
- З.5. Методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных.

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины

Максимальной учебной нагрузки обучающегося **72** часа, в том числе:

- обязательная аудиторная учебная нагрузка обучающегося **64 часа**;
- самостоятельная работа обучающегося **8 часов**.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	**72**
Обязательная аудиторная учебная нагрузка (всего)	**64**
в том числе:	
лекции	**32**
лабораторные занятия	—
практические занятия	**32**
курсовая работа (проект) (если предусмотрено)	—
Самостоятельная работа студента (всего)	**8**
в том числе:	
подготовка рефератов, докладов, презентаций	4
выполнение индивидуальных исследовательских заданий	4
Консультации	—
Промежуточная аттестация	**Зачет**

2.2. Тематический план и содержание учебной дисциплины «ОП.05 Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	В том числе часы по практической подготовке	Уровень освоения
Раздел 1. Основы информационной безопасности		**44**	**22**	
Тема 1.1. Введение в информационную безопасность	Содержание учебного материала (лекция)	2		2
	Лекция №1. Основные понятия и определения. История и развитие информационной безопасности.			
	Лекция №2. Актуальные угрозы и риски в информационной безопасности.			
	Практическое занятие №1. «Анализ актуальных угроз информационной безопасности» (анализ статистики кибератак, классификация угроз, составление перечня актуальных угроз для различных сфер деятельности).	2	2	2
	Самостоятельная работа №1. Подготовка аналитического обзора по теме: «Эволюция киберугроз за последние 10 лет».	1		3
Тема 1.2. Управление безопасностью информации	Содержание учебного материала (лекция)	2		2
	Лекция №3. Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности.			
	Лекция №4. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.).			
	Практическое занятие №2. «Оценка рисков информационной безопасности» (проведение оценки рисков для условной организации, определение угроз, уязвимостей, расчет уровня риска).	2	2	2
	Самостоятельная работа №2. Изучение нормативных документов (анализ требований Федерального закона «О персональных данных» (152-ФЗ) и его влияние на организационные меры защиты информации).	1		3
Тема 1.3. Криптография	Содержание учебного материала (лекция)	4		2
	Лекция №5. Основы криптографии. Симметричные алгоритмы шифрования.			

	Лекция №6. Асимметричные алгоритмы шифрования.			
	Лекция №7. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.			
	Практическое занятие №3. «Работа с симметричными и асимметричными алгоритмами» (работа с OpenSSL, GnuPG; шифрование и дешифрование данных).	2	2	2
	Практическое занятие №4. «Хэширование и создание цифровой подписи сообщения».	2	2	2
	Самостоятельная работа №3. Сравнительный анализ алгоритмов шифрования.	1		3
Тема 1.4. Защита сетевой инфраструктуры	Содержание учебного материала (лекция)	2		2
	Лекция №8. Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.).			
	Лекция №9. Использование VPN и межсетевых экранов.			
	Практическое занятие №5. «Организация защиты от атак. Настройка межсетевого экрана (брандмауэра)».	2	2	2
	Практическое занятие №6. «Организация работы VPN» (настройка VPN-соединения OpenVPN или WireGuard).	2	2	2
	Самостоятельная работа №4. Исследование протоколов VPN.	1		3
Тема 1.5. Безопасность приложений	Содержание учебного материала (лекция)	2		2
	Лекция №10. Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики.			
	Лекция №11. Тестирование на проникновение и анализ уязвимостей.			
	Практическое занятие №7. «Анализ уязвимостей веб-приложений».	2	2	2
	Самостоятельная работа №5. Изучение OWASP Top Ten.	1		3
Тема 1.6. Защита данных	Содержание учебного материала (лекция)	2		2
	Лекция №12. Шифрование данных в покое и в транзите.			
	Лекция №13. Резервное копирование и восстановление данных. Управление доступом к данным.			
	Практическое занятие №8. «Выполнение резервного	2	2	2

	копирования и восстановления данных».			
	Практическое занятие №9. «Управление доступом к данным».	2	2	2
	Самостоятельная работа №6. Разработка политики резервного копирования.	1		3
Тема 1.7. Безопасность облачных технологий	Содержание учебного материала (лекция)	2		2
	Лекция №14. Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS). Модели ответственности (Shared Responsibility Model).			
	Практическое занятие №10. «Изучение моделей облачных услуг и их безопасности».	2	2	2
	Самостоятельная работа №7. Анализ облачных провайдеров.	1		3
Тема 1.8. Инциденты безопасности	Содержание учебного материала (лекция)	2		2
	Лекция №15. Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика.			
	Практическое занятие №11. «Работа с инцидентами безопасности».	2	2	2
	Самостоятельная работа №8. Разработка плана реагирования на инциденты.	1		3
Тема 1.9. Социальная инженерия и человеческий фактор	Содержание учебного материала (лекция)	2		2
	Лекция №16. Психология атак: социальная инженерия. Методы и приемы социальных инженеров. Обучение сотрудников информационной безопасности.			
	Практическое занятие №12. «Разработка политики информационной безопасности».	2	2	2
	Самостоятельная работа №9. Создание памятки по противодействию социальной инженерии.	1		3
Тема 1.10. Будущее информационной безопасности	Содержание учебного материала (лекция)	2		2
	Лекция №17. Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности.			

	Практическое занятие №13. «Исследование современных тенденций в области ИБ».	2	2	2
	Самостоятельная работа №10. Подготовка исследовательского проекта.	1		3
Промежуточная аттестация	**Зачет**	**5**		
Всего:		**72**	**32**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

№ п/п	Наименование дисциплины (модуля), практик в соответствии с учебным планом	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	ОП.05 Основы информационной безопасности	Ауд. № 2.114 (78,0 м²) Мультимедийный зал научной библиотеки для самостоятельной работы с выходом в сеть Интернет	**Оборудование:** Системный блок Core quad q6600, 4GB RAM, 160GB HDD – 1 шт.; Монитор Benq G900WA – 1 шт.; Системный блок Deponeon core2duo e8300, 2GB RAM, 160GB HDD – 8 шт.; Монитор LG W1934S – 8 шт.; Тонкие клиенты Eltex TC-50 – 4 шт. **Учебная мебель:** Компьютерный стол – 15 шт., стол – 9 шт., стулья – 23 шт. **Программное обеспечение:** Бесплатная операционная система Calculate Linux; LIBREOFFICE (открытое лицензионное соглашение GNU General Public License).
2		Ауд. № 2.313 (52,5 м²) Компьютерный класс информационных технологий в профессиональной деятельности	**Оборудование:** АРМ на 14 обучающихся (NL Intel Core i3-10100/2×4Gb/GeForce RTX 3050/500Gb/Win10Pro/Office, монитор 23.8" AOC 24B2XHM2); АРМ преподавателя – 1 шт.; Проектор и экран – 1 комплект. **Учебная мебель:** Компьютерный стол – 16 шт., стул подъемно-поворотный – 1 шт., стулья со спинкой – 25 шт., шкаф для документов – 1 шт., доска трехэлементная (3000×1000×20) – 1 шт.
3		Ауд. № 2.406 Компьютерный класс. Лаборатория информационных ресурсов	**Оборудование:** АРМ обучающихся: системный блок (Rusco Core-i3-7100/2×4Gb/500Gb/Win10Pro/Office) – 15 шт., монитор (22" Benq GL2250) – 15 шт.; АРМ преподавателя – 1 шт.; Интерактивная доска SMART Board 680; Проектор LG RL-JT40; МФУ HP LaserJet Pro MFP 127fn – 1 шт.; навесной экран, маркерная доска. **Учебная мебель:** Специализированная мебель для сервисного обслуживания ПК с заземлением и защитой от статического напряжения, компьютерный стол – 16 шт., стул подъемно-поворотный – 16 шт., стулья – 25 шт.

3.2. Информационное обеспечение обучения

Перечень учебных изданий, интернет-ресурсов, дополнительной литературы

Основные источники:

№	Авторы, составители	Заглавие	Издательство, год
1	Баланов А. Н.	Защита информационных систем. Кибербезопасность : учебное пособие для СПО	Санкт-Петербург : Лань, 2025
2	Баланов А. Н.	Комплексная информационная безопасность : учебное пособие для СПО	Санкт-Петербург : Лань, 2025
3	Нестеров С. А.	Основы информационной безопасности : учебник для СПО	Санкт-Петербург : Лань, 2022
4	Прохорова О. В.	Информационная безопасность и защита информации : учебник для СПО	Санкт-Петербург : Лань, 2024

Дополнительная литература:

№	Авторы, составители	Заглавие	Издательство, год
1	Галатенко В. А.	Основы информационной безопасности	М.: Интернет-Университет Информационных Технологий, 2021
2	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей	М.: Форум, 2020

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

№	Наименование
1	Сайт Научной библиотеки АГАТУ — https://agatu.ru/lib/
2	Электронная обучающая оболочка Moodle — https://sdo.agatu.ru/
3	Официальный сайт Positive Technologies (раздел «Аналитика и исследования») — https://www.ptsecurity.com/ru-ru/research/
4	Официальный сайт «Лаборатории Касперского» (раздел «Библиотека знаний») — https://www.kaspersky.ru/resource-center
5	Ресурс OWASP (Open Web Application Security Project) — https://owasp.org/
6	Электронно-библиотечная система «Лань» — https://e.lanbook.com/
7	Электронно-библиотечная система «ЮРАЙТ» — https://urait.ru/

Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

№	Наименование
1	Операционная система Calculate Linux (свободно распространяемое)
2	LIBREOFFICE (открытое лицензионное соглашение GNU General Public License)
3	Microsoft Windows 10 Pro (лицензионное)
4	Microsoft Office (лицензионное)
5	OpenSSL (свободно распространяемое)
6	GnuPG (свободно распространяемое)
7	VirtualBox (свободно распространяемое)
8	Wireshark (свободно распространяемое)
9	Burp Suite Community Edition (свободно распространяемое)

Перечень профессиональных баз данных и информационных справочных систем

№	Наименование
1	Научная электронная библиотека eLIBRARY.RU — https://www.elibrary.ru
2	Официальный интернет-портал правовой информации — http://pravo.gov.ru
3	Справочно-правовая система «КонсультантПлюс»
4	Справочно-правовая система «Гарант»
5	База данных ФИПС (патенты, полезные модели) — https://www.fips.ru

3.3. Условия реализации учебной дисциплины для студентов-инвалидов и лиц с ограниченными возможностями здоровья

3.3.1. Образовательные технологии

С целью оказания помощи в обучении студентов-инвалидов и лиц с ОВЗ применяются образовательные технологии с использованием универсальных, специальных информационных и коммуникационных средств.

Для основных видов учебной работы применяются:

Контактная работа:

- лекции – проблемная лекция, лекция-дискуссия, лекция-диалог, лекция-консультация, лекция с применением дистанционных технологий и привлечением возможностей Интернета;
- практические занятия – практические задания;
- групповые консультации – опрос, работа с лекционным и дополнительным материалом;
- индивидуальная работа с преподавателем – индивидуальная консультация, работа с лекционным и дополнительным материалом, беседа, морально-эмоциональная поддержка и стимулирование, дистанционные технологии.

Формы самостоятельной работы устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге или на компьютере).

В качестве самостоятельной подготовки в обучении используется система дистанционного обучения **Moodle**.

Самостоятельная работа:

- работа с книгой и другими источниками информации, план-конспекты;
- творческие самостоятельные работы;
- дистанционные технологии.

При необходимости обучающимся предоставляется дополнительное время для консультаций и выполнения заданий.

3.3.2. Специальное материально-техническое и учебно-методическое обеспечение

При обучении по дисциплине используется система, поддерживающая дистанционное образование — **«Moodle»**, ориентированная на организацию дистанционных курсов, а также на организацию взаимодействия между преподавателем и обучающимися посредством интерактивных обучающих элементов курса.

Для обучающихся лиц с нарушением зрения предоставляются:

- видеоувеличитель-монокуляр для просмотра Levenhuk Wise 8×25;
- электронный ручной видеоувеличитель видео оптик «wu-tv»;
- возможно также использование собственных увеличивающих устройств;
- версия сайта академии http://www.agatu.ru/ для слабовидящих.

Для обучающихся лиц с нарушением слуха предоставляются:

- аудитории со звукоусиливающей аппаратурой (колонки, микрофон);
- компьютерная техника в оборудованных классах;
- учебные аудитории с мультимедийной системой с проектором;
- аудитории с интерактивными досками;
- учебные пособия, методические указания в форме электронного документа.

Для обучающихся лиц с нарушениями опорно-двигательного аппарата предоставляются:

- система дистанционного обучения Moodle;
- учебные пособия, методические указания в форме электронного документа.

3.3.3. Контроль и оценка результатов освоения учебной дисциплины

Контроль результатов обучения осуществляется в процессе проведения практических занятий, выполнения индивидуальных самостоятельных работ.

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации инвалидов и лиц с ОВЗ имеются фонды оценочных средств в ИС «Тестирование».

Формы и сроки проведения рубежного контроля определяются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.), и может проводиться в несколько этапов.

При необходимости предоставляется дополнительное время для подготовки ответов на зачете, аттестация проводится в несколько этапов (по частям), во время аттестации может присутствовать ассистент, аттестация прерывается для приема пищи, лекарств, во время аттестации используются специальные технические средства.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
Уметь:	
У.1. 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.	Экспертное наблюдение и оценка на практических занятиях. Оценка результатов выполнения практических работ (№1-13).
У.2. 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.	Защита отчетов по практическим работам. Оценка решений ситуационных задач.
У.3. Оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач.	Оценка качества оформления отчетов. Наблюдение за процессом работы с ПО в ходе практических занятий.
У.4. Понимать тексты на базовые профессиональные темы (на иностранном языке).	Устный опрос. Анализ терминологии в рамках профессиональных текстов.
У.5. Шифровать данные и обеспечивать их конфиденциальность.	Практические занятия №3, №4, №8. Оценка правильности выполнения заданий по шифрованию и защите данных.
Знать:	
З.1. 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.	Тестирование. Устный опрос.
З.2. Номенклатуру информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации.	Проверка рефератов (самостоятельная работа №1). Оценка структурированности отчетов по практическим работам.
З.3. Основные принципы и методы обеспечения безопасности информационных систем.	Зачет. Тестирование.
З.4. Принципы криптографии и методов шифрования данных; стандарты и протоколы безопасности (SSL/TLS, SSH, Kerberos, HTTPS, OAuth и др.).	Контрольная работа по теме «Криптография». Устный опрос.
З.5. Методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных.	Тестирование. Оценка выполнения практического задания по настройке прав доступа (ПЗ №9).
Итоговый контроль:	**Зачет**

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Арктический государственный агротехнологический университет»
Колледж технологий и управления

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине
ОП.05 Основы информационной безопасности
для обучающихся по специальности
09.02.11 Разработка и управление программным обеспечением

Якутск 2026 г

Фонд оценочных средств учебной дисциплины разработан в соответствии с:
- Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением, утвержденным приказом Министерства образования и науки Российской Федерации от 24.02.2025 № 138.
- Учебным планом специальности09.02.11 Разработка и управление программным обеспечением, одобренным Ученым советом ФГБОУ ВО Арктический ГАТУ от 02.04.2026 г. № 56.

Разработчик(и) ФОС Федоров Павел Иванович – преподаватель

Фонд оценочных средств учебной дисциплины ОП.05 Основы информационной безопасности одобрен Цикловой комиссией гуманитарных и естественных дисциплин от 13 марта 2026 г, протокол №10.

Председатель ЦК ГиЕД_____ _____ /Васильева Е.К./
подпись фамилия, имя, отчество

Фонд оценочных средств учебной дисциплины рассмотрен и рекомендован к использованию в учебном процессе на заседании методической комиссии Колледжа технологий и управления по специальности 09.02.11 Разработка и управление программным обеспечением.

Председатель методической комиссии КТиУ _____ /Ваганова В.Г./
подпись фамилия, имя, отчество