МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени В.Я.ГОРИНА»

УТВЕРЖДАЮ
И.о. декана инженерного факультета
кандидат технических наук, доцент
А.Н. Макаренко
27.05.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль): Прикладная информатика в АПК

Квалификация: бакалавр

Год начала подготовки: 2026

Майский, 2026

Рабочая программа дисциплины (модуля) составлена с учетом требований:

- федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 – Прикладная информатика, утвержденного приказом Министерства образования и науки РФ от 19 сентября 2017 г. № 922;
- порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства образования и науки РФ от 06.04.2021 № 245;
- профессионального стандарта «Специалист по информационным системам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н
- профессионального стандарта «Системный аналитик», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 27 апреля 2023 г. № 367н.

Составитель: к.т.н., доцент Миронов А.Л., сотрудник ООО «Русагро Тех» Виноградов Н. Д.

Рассмотрена на заседании методической комиссии инженерного факультета 27.05.2026 г., протокол №3-25/26

Председатель методической комиссии  Чехунов О.А.

Руководитель основной профессиональной образовательной программы  Мироненко А.В.

I. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цель дисциплины – ознакомление студентов с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации при проектировании информационных систем.

1.2. Задачи:

Задачи дисциплины заключаются в приобретение студентами прочных знаний и практических навыков в области, определяемой основной целью курса. В процессе изучения дисциплины студент должен получить представление о: международных стандартах информационного обмена; понятии угрозы; информационной безопасности в условиях функционирования в России глобальных сетей; видах противников или «нарушителей»; понятия о видах вирусов; видах возможных нарушений информационной системы; основных нормативных руководящих документах, касающиеся государственной тайны, нормативно-справочных документах; назначении и задачах в сфере обеспечения информационной безопасности на уровне государства; основных положениях теории информационной безопасности информационных систем; моделях безопасности и их применении; таксономии нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование; анализе способов нарушений информационной безопасности; использовании защищенных компьютерных систем; методах криптографии; основных технологиях построения защищенных ЭИС; месте информационной без- опасности экономических систем в национальной безопасности страны; концепции информационной безопасности.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ (ОПОП)

2.1. Цикл (раздел) ОПОП, к которому относится дисциплина

Информационная безопасность относится к дисциплинам обязательной части Б1.О.21 основной профессиональной образовательной программы.

2.2. Логическая взаимосвязь с другими частями ОПОП

Наименование предшествующих дисциплин, практик, на которых базируется данная дисциплина (модуль)	1. Математика
	2. Дискретная математика
	3. Алгоритмизация и программирование
Требования к предварительной подготовке обучающихся	***знать:*** ➢ основные понятия, используемые в информатике и программировании;

	➢ элементарные методы математики, экономико-статистические методы исследования; ➢ понятия системы и системного анализа; ***уметь:*** ➢ применять средства компьютерной техники, пакеты прикладных программ для решения прикладных задач; ➢ пользоваться сетевыми информационными ресурсами, работать с сетевыми службами и сервисами; ***владеть:*** ➢ навыками использования офисных прикладных программ и информационных ресурсов сети Интернет

Освоение дисциплины «Информационная безопасность» необходимо для изучения других дисциплин профессионального цикла, а также для выполнения ВКР.

III. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Коды компетенций	Формулировка компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.1** Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности **ОПК-3.2** Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности **ОПК-3.3** Демонстрирует навыки подготовки обзоров, анно-	**Знать:** основные требования информационной безопасности при решении стандартных задач профессиональной деятельности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации **Уметь:** выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации. **Владеть:** навыками обеспечения безопасного использования информационно-коммуникационных технологий, применения способов и средств защиты информации

		таций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	

IV. ОБЪЕМ, СТРУКТУРА, СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, ВИДЫ УЧЕБНОЙ РАБОТЫ И ФОРМЫ КОНТРОЛЯ ЗНАНИЙ

4.1. Распределение объема учебной работы по формам обучения

Вид работы (в соответствии с учебным планом)	**Объем учебной работы, час**	
Формы обучения (вносятся данные по реализуемым формам)	**Очная**	
Семестр изучения дисциплины	**6**	
Общая трудоемкость, всего, час *зачетные единицы*	*180* *5*	
1.Контактная работа		
1.1.Контактная аудиторная работа *(всего)*	**66,4**	
В том числе:		
Лекции *(Лек)*	16	
Лабораторные занятия *(Лаб)*	32	
Практические занятия *(Пр)*	32	
Установочные занятия *(УЗ)*	-	
Предэкзаменационные консультации *(Конс)*	2	
1.2.Промежуточная аттестация		
Зачет *(КЗ)*	-	-
Экзамен *(КЭ)*	0,4	
Выполнение курсовой работы (проекта) (*КНКР*)	-	
Выполнение контрольной работы *(ККН)*	-	
1.3.Контактная внеаудиторная работа *(контроль)*	**16**	
2. Самостоятельная работа обучающихся (всего)	**97,6**	
в том числе:		
Самостоятельная работа по проработке лекционного материала	10	
Самостоятельная работа по подготовке к лабораторно-практическим занятиям	40	
Работа над темами (вопросами), вынесенными на самостоятельное изучение	21,6	
Самостоятельная работа по видам индивидуальных заданий : подготовка реферата (контрольной работы)	10	
Подготовка к экзамену	16	

4.2 Общая структура дисциплины и виды учебной работы

Наименование модулей и разделов дисциплины	Объемы видов учебной работы по формам обучения, час								
	Очная форма обучения								
	Всего	**Лекции**	**Лабораторно-практ.занятия**		**Самостоятельная работа**				
1	2	3	4		6				
Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»	**48**	**4**	**4**	**10**	**30**				
1. Современный ландшафт киберугроз и триада информационной безопасности (*CIA-триада: конфиденциальность, целостность, доступность*) в эпоху цифровой трансформации.	6	1			5				
2. Построение системы управления информационной безопасностью (*СУИБ/ISMS*): процессы, метрики эффективности (*KPI*) и жизненный цикл защиты.	9	1	1	2	5				
3. Комплаенс-ориентированная безопасность: ФЗ-152, ФЗ-187, *ГОСТ Р 57580*, а также международные фреймворки (*ISO/IEC 27001*, *NIST CSF*) и их интеграция.	4	1	1	2	10				
4. Управление кибербезопасностью на уровне бизнеса: классификация активов, моделирование актуальных угроз (*ФСТЭК*, *MITRE ATT&CK*) и оценка рисков.	6	1	1	4	10				
Итоговое занятие по модулю 1	3	-	*1*	*2*					
Модуль 2 «Вирусы и удаленные угрозы в сетях»	**52**	**6**	**6**	**10**	**30**				
1. Современная таксономия вредоносного ПО: шифровальщики (*Ransomware*), шпионское ПО, банковские трояны, *APT-фреймворки*. Тактика злоумышленников по матрице *MITRE ATT&CK*.	9	1	1	2	5				
2. Проактивная защита конечных точек (*EDR/XDR*, песочницы). Поведенческий анализ, противодействие бесфайловым атакам (*fileless*) и техникам обхода антивирусов *(BYOVD — Bring Your Own Vulnerable Driver)*.	10	1	2	2	5				
3. Безопасность современных сетей: сегментация (*VLAN*, микросегментация), SDN (*Software-Defined Networking*), безопасность контейнеров (*Service Mesh*) и API-шлюзов.	15	2	1	2	10				

4. Анализ сетевого трафика и обнаружение вторжений (*IDS/IPS*, NTA). Защита от DDoS уровня L3-L7. Угрозы прикладного уровня (*Web Application Firewall*, OWASP Top 10). IPv6-безопасность и атаки на протоколы маршрутизации (*BGP Hijacking*).	15	2	1	2	10				
Итоговое занятие по модулю 2	3		*1*	*2*					
Модуль 3 «Принципы и методы защиты в вычислительных сетях»	**67,6**	**6**	**6**	**12**	**37,6**				
1. Безопасность современных распределенных систем: уязвимости микросервисной архитектуры и публичных *API* (*REST*, *GraphQL*). Атаки на цепочку поставок ПО (*Supply Chain Attacks*) через зависимости (*npm/pip*) и образы контейнеров (*Docker Hub*). Анализ причин: небезопасные конфигурации облаков (*S3*-buckets), отсутствие валидации входных данных.	15	2	1	2	9				
2. Архитектура безопасного приложения: идентификация без пароля (*Passwordless Auth*, биометрия, *Passkeys/FIDO2*). Использование протоколов централизованной авторизации (*OAuth 2.0*, *OpenID Connect*) и внедрение ролевой модели доступа (*RBAC/ABAC*) непосредственно в логику приложения. Безопасная работа сервисных учетных записей (*Service Accounts*).	17	2	1	2	9				
3. Мониторинг безопасности приложений (*AppSec*): отладка и безопасный вывод логов (почему нельзя писать пароли и токены в stdout). Внедрение *SIEM* для анализа событий приложения. Защита *API Gateway*. Межсетевое экранирование уровня приложения (*WAF*) и его настройка под конкретные фреймворки.	16	1	2	4	9,6				
4. Прикладная криптография для разработчика: безопасное хранение секретов пользователей (хеширование bcrypt/argon2, добавление соли). Шифрование данных в приложении, защита строк подключения к БД и конфигурационных файлов. Разграничение доступа на уровне строк базы данных (*Row-Level Security*) и полей объекта. Основы постквантовой криптографии (*PQC*).	16,6	1	2	4	9				
Итоговое занятие по модулю 3	3		*1*	*2*					
Выполнение контрольной работы (ККН)									
Предэкзаменационные консультации	***2***								
Установочные занятия	***-***								
Промежуточная аттестация	***0,4***								
Контроль	***16***								
Контактная аудиторная работа (всего)	***66,4***	***16***	***1 6***	***3 2***	***-***				
Контактная внеаудиторная работа (всего)	***16***								
Самостоятельная работа (всего)	***97,6***								
Общая трудоемкость	***180***								

4.3 Содержание дисциплины

Наименование и содержание модулей и разделов дисциплины
Модуль 1 **«Составляющие, уровни обеспечения и угрозы ИБ»**
1. Современный ландшафт киберугроз и триада информационной безопасности (*CIA-триада: конфиденциальность, целостность, доступность*) в эпоху цифровой трансформации.
2. Построение системы управления информационной безопасностью (*СУИБ/ISMS*): процессы, метрики эффективности (*KPI*) и жизненный цикл защиты.
3. Комплаенс-ориентированная безопасность: ФЗ-152, ФЗ-187, *ГОСТ Р 57580*, а также международные фреймворки (*ISO/IEC 27001*, *NIST CSF*) и их интеграция.
4. Управление кибербезопасностью на уровне бизнеса: классификация активов, моделирование актуальных угроз (*ФСТЭК*, *MITRE ATT&CK*) и оценка рисков.
Итоговое занятие по модулю 1
Модуль 2 **«Вирусы и удаленные угрозы в сетях»**
1. Современная таксономия вредоносного ПО: шифровальщики (*Ransomware*), шпионское ПО, банковские трояны, *APT-фреймворки*. Тактика злоумышленников по матрице *MITRE ATT&CK*.
2. Проактивная защита конечных точек (*EDR/XDR*, песочницы). Поведенческий анализ, противодействие бесфайловым атакам (*fileless*) и техникам обхода антивирусов *(BYOVD — Bring Your Own Vulnerable Driver)*.
3. Безопасность современных сетей: сегментация (*VLAN*, микросегментация), SDN (*Software-Defined Networking*), безопасность контейнеров (*Service Mesh*) и API-шлюзов.
4. Анализ сетевого трафика и обнаружение вторжений (*IDS/IPS*, NTA). Защита от DDoS уровня L3-L7. Угрозы прикладного уровня (*Web Application Firewall*, OWASP Top 10). IPv6-безопасность и атаки на протоколы маршрутизации (*BGP Hijacking*).
Итоговое занятие по модулю 2
Модуль 3 **«Принципы и методы защиты в вычислительных сетях»**
1. Безопасность современных распределенных систем: уязвимости микросервисной архитектуры и публичных *API* (*REST*, *GraphQL*). Атаки на цепочку поставок ПО (*Supply Chain Attacks*) через зависимости (*npm/pip*) и образы контейнеров (*Docker Hub*). Анализ причин: небезопасные конфигурации облаков (*S3*-buckets), отсутствие валидации входных данных.
2. Архитектура безопасного приложения: идентификация без пароля (*Passwordless Auth*, биометрия, *Passkeys/FIDO2*). Использование протоколов централизованной авторизации (*OAuth 2.0*, *OpenID Connect*) и внедрение ролевой модели доступа (*RBAC/ABAC*) непосредственно в логику приложения. Безопасная работа сервисных учетных записей (*Service Accounts*).
3. Мониторинг безопасности приложений (*AppSec*): отладка и безопасный вывод логов (почему нельзя писать пароли и токены в stdout). Внедрение *SIEM* для анализа событий приложения. Защита *API Gateway*. Межсетевое экранирование уровня приложения (*WAF*) и его настройка под конкретные фреймворки.
4. Прикладная криптография для разработчика: безопасное хранение секретов пользователей (хеширование bcrypt/argon2, добавление соли). Шифрование данных в приложении, защита строк подключения к БД и конфигурационных файлов. Разграничение доступа на уровне строк базы данных (*Row-Level Security*) и полей объекта. Основы постквантовой криптографии (*PQC*).
Итоговое занятие по модулю 3
Подготовка реферата в форме презентации (контрольной работы)
Зачет

V. ОЦЕНКА ЗНАНИЙ И ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1. Формы контроля знаний, рейтинговая оценка и формируемые компетенции (очная форма обучения)

№ п/п	Наименование рейтингов, модулей и блоков	Формируемые компетенции	Объем учебной работы				Форма контроля знаний	Количество баллов (min)	Количество баллов (max)
			Общая трудоемкость	Лекции	Лабор.-практ.занятия	Самост. работа			
Всего по дисциплине		***ОПК-3.1 ОПК-3.2 ОПК-3.3***	**180**	**16**	**48**	**97,6**	**Зачет**	**51**	**100**
I. Рубежный рейтинг							Сумма баллов за модули	***31***	***60***
Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»		***ОПК-3.1 ОПК-3.2 ОПК-3.3***	**48**	**4**	**4**	**10**		**10**	**20**
1.	Современный ландшафт киберугроз и триада информационной безопасности (*CIA-триада: конфиденциальность, целостность, доступность*) в эпоху цифровой трансформации.		6	1			Устный опрос		
2.	Построение системы управления информационной безопасностью (*СУИБ/ISMS*): процессы, метрики эффективности (*KPI*) и жизненный цикл защиты.		9	1	1	2	Устный опрос		
3.	Комплаенс-ориентированная безопасность: ФЗ-152, ФЗ-187, *ГОСТ Р 57580*, а также международные фреймворки (*ISO/IEC 27001*, *NIST CSF*) и их интеграция.		4	1	1	2	Устный опрос		
4	Управление кибербезопасностью на уровне бизнеса: классификация активов, моделирование актуальных угроз (*ФСТЭК*, *MITRE ATT&CK*) и оценка рисков.		6	1	1	4	Устный опрос		
	Итоговый контроль знаний по темам модуля 1		3	-	*1*	*2*	Устный опрос, тестирование		

Модуль 2. **«Вирусы и удаленные угрозы в сетях»**		***ОПК-3.1*** ***ОПК-3.2*** ***ОПК-3.3***	**52**	**6**	**6**	**10**		**10**	**20**
1.	Современная таксономия вредоносного ПО: шифровальщики (*Ransomware*), шпионское ПО, банковские трояны, *APT-фреймворки*. Тактика злоумышленников по матрице *MITRE ATT&CK*.		9	1	1	2	Устный опрос		
2.	Проактивная защита конечных точек (*EDR/XDR*, песочницы). Поведенческий анализ, противодействие бесфайловым атакам (*fileless*) и техникам обхода антивирусов *(BYOVD — Bring Your Own Vulnerable Driver)*.		10	1	2	2	Устный опрос		
3.	Безопасность современных сетей: сегментация (*VLAN*, микросегментация), SDN (*Software-Defined Networking*), безопасность контейнеров (*Service Mesh*) и API-шлюзов.		15	2	1	2	Устный опрос		
4.	Анализ сетевого трафика и обнаружение вторжений (*IDS/IPS*, NTA). Защита от DDoS уровня L3-L7. Угрозы прикладного уровня (*Web Application Firewall*, OWASP Top 10). IPv6-безопасность и атаки на протоколы маршрутизации (*BGP Hijacking*).		15	2	1	2	Устный опрос		
	Итоговый контроль знаний по темам модуля 2.		3		*1*	*2*	Устный опрос, тестирование		
Модуль 3 **«Принципы и методы защиты в вычислительных сетях»**		***ОПК-3.1*** ***ОПК-3.2*** ***ОПК-3.3***	**67,6**	**6**	**6**	**12**		**11**	**20**
1.	Безопасность современных распределенных систем: уязвимости микросервисной архитектуры и публичных *API* (*REST*, *GraphQL*). Атаки на цепочку поставок ПО (*Supply Chain Attacks*) через зависимости (*npm/pip*) и образы контейнеров (*Docker Hub*). Анализ причин: небезопасные конфигурации облаков (*S3*-buckets), отсутствие валидации входных данных.		15	2	1	2			
2.	Архитектура безопасного приложения: идентификация без пароля (*Passwordless Auth*, биометрия, *Passkeys/FIDO2*). Использование протоколов централизованной авторизации (*OAuth 2.0*, *OpenID Connect*) и внедрение ролевой модели доступа (*RBAC/ABAC*) непосредственно в логику приложения. Безопасная работа сервисных учетных записей (*Service Accounts*).		17	2	1	2			

3.	Мониторинг безопасности приложений (*AppSec*): отладка и безопасный вывод логов (почему нельзя писать пароли и токены в stdout). Внедрение *SIEM* для анализа событий приложения. Защита *API Gateway*. Межсетевое экранирование уровня приложения (*WAF*) и его настройка под конкретные фреймворки.		16	1	2	4			
4.	Прикладная криптография для разработчика: безопасное хранение секретов пользователей (хеширование bcrypt/argon2, добавление соли). Шифрование данных в приложении, защита строк подключения к БД и конфигурационных файлов. Разграничение доступа на уровне строк базы данных (*Row-Level Security*) и полей объекта. Основы постквантовой криптографии (*PQC*).		16,6	1	2	4			
	Итоговый контроль знаний по темам модуля 3.		3		*1*	*2*	Устный опрос, тестирование		
	II. Творческий рейтинг							**2**	**5**
	III. Рейтинг личностных качеств							**3**	**10**
	IV . Рейтинг сформированности прикладных практических требований							+	+
	V. Промежуточная аттестация							**15**	**25**

*Указана трудоемкость без учета внеаудиторной работы и промежуточной аттестации

5.2. Оценка знаний студента

5.2.1. Основные принципы рейтинговой оценки знаний

Оценка знаний по дисциплине осуществляется согласно положению «О единых требованиях к контролю и оценке результатов обучения: Методические рекомендации по практическому применению модульно-рейтинговой системы обучения».

Уровень развития компетенций оценивается с помощью рейтинговых баллов.

Рейтинги	**Характеристика рейтингов**	**Максимум баллов**
Рубежный	Отражает работу студента на протяжении всего периода изучения дисциплины. Определяется суммой баллов, которые студент получит по результатам изучения каждого модуля.	60
Творческий	Результат выполнения студентом индивидуального творческого задания различных уровней сложности, в том числе, участие в различных конференциях и конкурсах на протяжении всего курса изучения дисциплины.	5
Рейтинг личностных качеств	Оценка личностных качеств обучающихся, проявленных ими в процессе реализации дисциплины (модуля) (дисциплинированность, посещаемость учебных занятий, сдача вовремя контрольных мероприятий, ответственность, инициатива и др.)	10
Рейтинг сформированности прикладных практических требований	Оценка результата сформированности практических навыков по дисциплине (модулю), определяемый преподавателем перед началом проведения промежуточной аттестации и оценивается как «зачтено» или «не зачтено».	+
Промежуточная аттестация	Является результатом аттестации на окончательном этапе изучения дисциплины по итогам сдачи зачета или экзамена. Отражает уровень освоения информационно-теоретического компонента в целом и основ практической деятельности в частности.	25
Итоговый рейтинг	Определяется путём суммирования всех рейтингов	100

Итоговая оценка компетенций студента осуществляется путём автоматического перевода баллов общего рейтинга в стандартные оценки:

Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
менее 51 балла	51-67 баллов	67,1-85 баллов	85,1-100 баллов

5.3. Фонд оценочных средств. Типовые контрольные задания или иные материалы, необходимые для оценки формируемых компетенций по дисциплине (приложение 2)

VI. УЧЕБНО - МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Основная учебная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 (дата обращения: 28.04.2023). – Режим доступа: по подписке.

6.2 Дополнительная литература

1. Миронов, А.Л. Информационная безопасность: Учебное пособие[Текст]/ А.Л. Миронов // Изд. Белгородского ГАУ, 2014. – 46 с.

6.3. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов заключается в инициативном поиске информации о наиболее актуальных проблемах, которые имеют большое практическое значение и являются предметом научных дискуссий в рамках изучаемой дисциплины.

Самостоятельная работа планируется в соответствии с календарными планами рабочей программы по дисциплине и в методическом единстве с тематикой учебных аудиторных занятий.

Самостоятельную работу студента поддерживает электронная информационная среда ВУЗа, доступ к которой http://do.belgau.edu.ru (логин, пароль студента)

6.3.1. Методические указания по освоению дисциплины

УМК по дисциплине – Режим доступа: https://do.belgau.ru

6.3.2. Видеоматериалы

Каталог учебных видеоматериалов на официальном сайте ФГБОУ ВО Белгородский ГАУ – Режим доступа: https://www.belgau.ru/InfResource/library/video/mehanizatsiya.php

6.3.3. Печатные периодические издания

1. Журнал «Информационные технологии».
2. Журнал «Моделирование и анализ информационных систем».
3. Журнал «Information Security. Информационная безопасность».

6.4. Ресурсы информационно-телекоммуникационной сети «Интернет», современные профессиональные базы данных, информационные справочные системы

Электронные ресурсы свободного доступа	
http://elibrary.ru/defaultx.asp	Всероссийский институт научной и технической информации
http://www2.viniti.ru	Научная электронная библиотека
https://mcx.gov.ru	Министерство сельского хозяйства РФ
http://www.ras.ru/	Российская Академия наук: структура РАН; инновационная и научная деятельность; новости, объявления, пресса.
http://www.cnshb.ru/	Центральная научная сельскохозяйственная библиотека
http://www.rsl.ru	Российская государственная библиотека
http://www.edu.ru	Российское образование. Федеральный портал
Ресурсы ФГБОУ ВО Белгородский ГАУ	
http://lib.belgau.ru	Электронные ресурсы библиотеки ФГБОУ ВО Белгородский ГАУ
http://ebs.rgazu.ru/	Электронно-библиотечная система (ЭБС) "AgriLib"
http://znanium.com/	ЭБС «ZNANIUM.COM»
http://e.lanbook.com/books/	Электронно-библиотечная система издательства «Лань»
http://www.garant.ru/	Информационное правовое обеспечение «Гарант» (для учебного процесса)
http://www.consultant.ru	СПС Консультант Плюс: Версия Проф

Вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Лабораторно-практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой

Вид учебных занятий	Организация деятельности студента
	литературы, работа с текстом (методика полевого опыта), решение задач по алгоритму и решение ситуационных задач Прослушивание аудио- и видеозаписей по заданной теме.
Самостоятельная работа	Знакомство с электронной базой данных кафедры морфологии и физиологии, основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др. Решение ситуационных задач по своему индивидуальному варианту, в которых обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы. Тестирование - система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Контрольная работа - средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.
Подготовка к экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, полученные навыки по решению ситуационных задач

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Помещения, укомплектованные специализированной мебелью, оснащенные оборудованием и техническими средствами обучения, служащими для представления учебной информации большой аудитории

Виды помещений	Оборудование и технические средства обучения
Учебная аудитория для проведения занятий лекционного типа №3	Специализированная мебель на 100 посадочных мест, доска настенная, кафедра, рабочее место преподавате-ля. Состав оборудования рабочего места: проектор EPSON EB-X18, экран для проектора с электроприводом Screen Media (моторизированный), колонки Microlab, ящик под проектор, ящик под кабели, ноут-бук преподавателя.
Учебная лаборатория «Прикладной информатики и информационных технологий» № 312	компьютер в сборе (15 комплектов) **комплект:** проектор Sony; интерактивная доска; настенно-потолочный кронштейн; кабель-монитор SVGA 5м; кабель монитор SVGA 3м; кабель Gembird 3м Ноутбук Lenovo Idea Pad 100-15 Стол ученический, стул ученический, стул вертушка, доска меловая настенная, стенд, жалюзи, купольная видеокамера
Помещение для хранения и	Специализированная мебель на 13 посадочных мест, доска магнитная,

профилактического обслуживания учебного оборудования	поворотная со стойкой, магниты в комплекте, кафедра, рабочее место преподавателя. Оборудование: компьютер (системный блок, монитор клавиатура мышь), МФУ BROTHER (принтер, сканер, ксерокс), принтер лазерный XEROX.
Помещения для самостоятельной работы (читальные залы библиотеки)	Читальный зал (вход №009) на 37 посадочных мест с возможностью бесплатного подключения к Интернету через Wi-Fi и обеспечением доступа в электронную информационно-образовательную среду Белгородского ГАУ. *Оборудование рабочего места библиотекаря:* - комплект компьютерной техники (системный блок, монитор, клавиатура, мышь) возможностью подключения к Интернету и обеспечением доступа в электронную информационно-образовательную среду Белгородского ГАУ; *Набор демонстрационного оборудования*: - настенный плазменный телевизор SAMSUNG PS50C450B1 Black HD (диагональ 127 см); - аудио-видео кабель HDMI (для подключения телевизора к компьютеру). Читальный зал (вход №012) на 80 посадочных мест с возможностью бесплатного подключения к Интернету через Wi-Fi и обеспечением доступа в электронную информационно-образовательную среду Белгородского ГАУ, в том числе 10 мест, оснащенных комплектами компьютерной техники (системный блок, монитор, клавиатура, мышь) с возможностью подключения к Интернету и обеспечением доступа в электронную информационно-образовательную среду Белгородского ГАУ. *Оборудование рабочего места библиотекаря:* библиотечная кафедра-стойка на три рабочих места; комплект компьютерной техники (системный блок, монитор, клавиатура, мышь) с возможностью подключения к Интернету и обеспечением доступа в электронную информационно-образовательную среду Белгородского ГАУ.

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

Виды помещений	Оборудование
Учебная аудитория для проведения занятий лекционного типа №3	- MS Windows WinStrtr 7 Acdmc Le-galization RUS OPL NL. ДоговорNo180 от12.02.2011. Срок дей-ствия лицензии –бессрочно; - MS Office Std 2010 RUS OPL NL Acdmc. Договор No180 от12.02.2011. Срок действия лицензии – бессрочно; Anti-virus Kaspersry Endpoint Security для бизнеса (Сублицензионный договор от 10.12.2025 № 20091042712510057l-4.0.25.1126) – 522 лицензии. Срок действия лицензии 1 год.
Учебная лаборатория «Прикладной информатики и информационных технологий» № 312	- MS Office Std 2010 RUS OPL NL Acdmc. Договор No180 от12.02.2011. Срок действия лицензии – бессрочно; Anti-virus Kaspersry Endpoint Security для бизнеса (Сублицензионный договор от 10.12.2025 № 20091042712510057l-4.0.25.1126) – 522 лицензии. Срок действия лицензии 1 год. - Информационно правовое обеспечение «Гарант» (для учебного процесса). Договор №ЭПС-12-119 от 01.09.2012. Срок действия - бессрочно. (отечественное ПО) - СПС КонсультантПлюс: Версия Проф. Консультант Финансист. КонсультантПлюс: Консультации для бюджетных организаций. Договор от 01.01.2017. Срок действия - бессрочно (отечественное ПО)
Помещение для хранения и профилактического обслуживания учебного оборудования	MS Office Std 2010 RUS OPL NL Acdmc. Договор №180 от 12.02.2011. Срок действия лицензии – бессрочно. Anti-virus Kaspersry Endpoint Security для бизнеса (Сублицензионный договор от 10.12.2025 № 20091042712510057l-4.0.25.1126) – 522 лицензии. Срок действия лицензии 1 год.
Помещения для самостоя-	– Microsoft Imagine Premium Electronic Software Delivery. Субли-

тельной работы (читальные залы библиотеки)	цензионный договор на передачу неисключительных прав №26 от 26.12.2019 . Срок действия- бессрочно – Информационно правовое обеспечение «Гарант» (для учебного процесса). Договор №ЭПС-12-119 от 01.09.2012. Срок действия – бессрочно. *(отечественное ПО)* – СПС КонсультантПлюс: Версия Проф. Консультант Финансист. КонсультантПлюс: Консультации для бюджетных организаций. Договор от 01.01.2017. Срок действия – бессрочно *(отечественное ПО)*

7.3. Электронные библиотечные системы и электронная информационно-образовательная среда

– ЭБС «ZNANIUM.COM», лицензионный договор (неисключительная лицензия) № 409эбс от 30.06.2025 с Обществом с ограниченной ответственностью «ЗНАНИУМ»;

– ЭБС «AgriLib», дополнительное соглашение № 1 от 31.01.2020/33 к лицензионному договору №ПДД 3/15 на предоставление доступа к электронно-библиотечной системе ФГБОУ ВПО РГАЗУ от 15.01.2015;

– ЭБС «Лань», лицензионный договор № 1-14-2025 от 06.10.2025 с Обществом с ограниченной ответственностью «Издательство Лань».

VIII. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае обучения в университете инвалидов и лиц с ограниченными возможностями здоровья учитываются особенности психофизического развития, индивидуальные возможности и состояние здоровья таких обучающихся.

Образование обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с ограниченными возможностями здоровья по слуху возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий). На аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и (или) тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста н списка литерату-

ры, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с ограниченными возможностями здоровья по зрению университетом обеспечивается выпуск и использование на учебных занятиях альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы) а также обеспечивает обучающихся надлежащими звуковыми средствами воспроизведения информации (диктофонов и т.д.). Допускается присутствие ассистента, оказывающего обучающемуся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно- двигательного аппарата материально-технические условия университета обеспечивают возможность беспрепятственного доступа обучающихся в учебные помещения, а также пребывания в них (наличие пандусов, поручней, расширенных дверных проемов, лифтов; наличие специальных кресел и других приспособлений). На аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации лицам с ограниченными возможностями здоровья, имеющим нарушения опорно-двигательного аппарата могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем)