	Министерство просвещения Российской Федерации
	Федеральное государственное бюджетное образовательное учреждение высшего образования «Армавирский государственный педагогический университет»
П-1-29-10-26	Локальные нормативные акты, регламентирующие общие положения
	Политика информационной безопасности в федеральном государственном бюджетном образовательном учреждении высшего образования «Армавирский государственный педагогический университет»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00CE6439D909A541A05A096BEB9AAA1F99
Владелец: Нижник Евгений Алексеевич
Действителен: с 25.11.2025 до 18.02.2027

«УТВЕРЖДАЮ»
Ректор ФГБОУ ВО «АГПУ»
_____ Е.А. Нижник
«____» _____ 2026 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «АРМАВИРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Д-1-32-10-26

Армавир, 2026

Рассмотрен ППО работников и обучающихся ФГБОУ ВО «АГПУ» общероссийского Профсоюза образования	*Протокол №13 от «16» октября 2026 г.*
Рассмотрен студенческим советом ФГБОУ ВО «АГПУ»	*Протокол № 2 от «13» октября 2026 г.*
Рассмотрен советом родителей (законных представителей) несовершеннолетних обучающихся ФГБОУ ВО «АГПУ»	*Протокол № 2 от «14» октября 2026 г.*
Принят (утвержден) ученым советом ФГБОУ ВО «АГПУ»	*Протокол № 18 от «23» октября 2026г.*
Регистрационный номер по журналу учета, дата регистрации	*№ 32 от «23» октября 2026г.*
Д-1-32-10-26	Стр. 1 из 6

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности (далее — Политика) устанавливает цели, принципы и основные направления деятельности по обеспечению информационной безопасности в федеральном государственном бюджетном образовательном учреждении высшего образования «Армавирский государственный педагогический университет» (далее — Университет).

1.2. Политика разработана с учётом требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Указа Президента Российской Федерации от 01.05.2022 № 250, приказа ФСТЭК России от 11.04.2025 № 117, приказа ФСТЭК России от 18.02.2013 № 21, а также иных нормативных правовых актов, применимых к информационным системам и ресурсам Университета.

1.3. Политика распространяется на все структурные подразделения Университета, всех работников, обучающихся и иных лиц, имеющих доступ к информационным ресурсам Университета.

1.4. Политика является основополагающим документом системы обеспечения информационной безопасности Университета. Ей подчинены иные локальные нормативные акты в области информационной безопасности (далее — ИБ): Регламент реагирования на компьютерные инциденты, Положение об обработке и защите персональных данных (является документом, определяющим политику Университета в отношении обработки персональных данных в соответствии с частью 2 статьи 18.1 Федерального закона № 152-ФЗ), Положение о кадровом электронном документообороте, Регламент по использованию электронной подписи при использовании кадрового эл.документооборота ФГБОУ ВО АГПУ.

2. ЦЕЛИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Целями обеспечения информационной безопасности являются:

– защита информационных ресурсов Университета от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, распространения;

– обеспечение непрерывности функционирования информационных систем, обеспечивающих образовательную, научную, финансово-хозяйственную деятельность Университета;

– выполнение применимых требований законодательства Российской Федерации в области защиты информации и персональных данных;

– минимизация рисков финансовых, репутационных и правовых потерь, связанных с нарушением информационной безопасности.

2.2. Обеспечение информационной безопасности в Университете основывается на принципах:

конфиденциальности — доступ к информации предоставляется только уполномоченным лицам;

целостности — информация защищается от несанкционированного изменения или уничтожения;

доступности — информация и информационные системы доступны уполномоченным лицам в необходимое время;

законности — все меры защиты информации применяются в соответствии с законодательством Российской Федерации;

экономической целесообразности — уровень затрат на защиту информации соразмерен ценности защищаемых активов и рискам;

использования отечественных сертифицированных средств защиты информации в соответствии с пунктом 6 Указа Президента Российской Федерации от 01.05.2022 № 250.

3. КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ АКТИВОВ

3.1. Информационные активы Университета подразделяются на следующие категории:

Категория	**Примеры**	**Правовой режим**
Информационные системы и сети Университета	ИС приёмной комиссии, ИС управления образовательным процессом, ИТКС Университета, СЭД, СКУД и видеонаблюдение, финансово-экономическая ИС, ЭИОС	149-ФЗ, 152-ФЗ и иные применимые нормативные правовые акты
Персональные данные	Данные сотрудников, обучающихся, абитуриентов	152-ФЗ
Государственные информационные системы	ФИС ФРДО, Суперсервис «Поступление в вуз онлайн», Витрина данных «Контингент студентов»	Отраслевые нормативные правовые акты, требования операторов соответствующих ГИС
Служебная и финансовая информация	Бухгалтерская, кадровая документация, договоры	Внутренние акты, 402-ФЗ
Кадровые электронные документы	Приказы, заявления, согласия в системе КЭДО	ТК РФ, 63-ФЗ

4. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ОБЕСПЕЧЕНИЯ ИБ

4.1. Общее руководство обеспечением информационной безопасности Университета осуществляется ректором. Координация деятельности структурных подразделений в сфере информационной безопасности возлагается на проректора по безопасности в пределах полномочий, закреплённых распорядительными актами Университета.

4.2. Организационно-методическое сопровождение мероприятий по защите информации, анализ угроз и подготовка предложений по совершенствованию защиты

осуществляются главным специалистом по защите информации в пределах полномочий, определённых должностной инструкцией и распорядительными актами Университета.

4.3. Руководители структурных подразделений организуют выполнение установленных требований информационной безопасности в своих подразделениях, обеспечивают участие работников в предусмотренных мероприятиях и своевременное сообщение о выявленных нарушениях.

4.4. Работники и иные лица, допущенные к информационным ресурсам Университета, обязаны соблюдать установленные требования информационной безопасности и сообщать о выявленных нарушениях в порядке, установленном локальными нормативными актами Университета.

4.5. Конкретные ответственные лица, распределение исполнительских и контрольных функций, полномочия по взаимодействию с государственными органами, а также порядок выполнения и проверки мероприятий по защите информации определяются отдельными приказами и регламентами Университета. При организации внутреннего контроля учитывается необходимость разграничения проверяемой деятельности и её оценки.

5. ОСНОВНЫЕ ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ

5.1. Доступ к информационным системам предоставляется только на основании приказа о допуске, с использованием индивидуальных учётных записей. Использование общих (групповых) учётных записей не допускается, за исключением технологических учётных записей, применение которых обосновано и документально зафиксировано.

5.2. Пароли должны соответствовать требованиям сложности, устанавливаемым отдельным регламентом. Передача паролей третьим лицам, хранение паролей в открытом виде на бумажных или электронных носителях не допускается.

5.3. Для защиты информационных систем применяются сертифицированные ФСТЭК России и (или) ФСБ России средства защиты информации, включённые в реестр российского программного обеспечения. Использование средств защиты информации производства государств, совершающих в отношении Российской Федерации недружественные действия, не допускается (п. 6 Указа Президента Российской Федерации № 250).

5.4. На всех автоматизированных рабочих местах и серверах Университета устанавливаются и поддерживаются в актуальном состоянии сертифицированные средства антивирусной защиты с централизованным управлением.

5.5. Критически важные информационные системы (финансово-экономическая система, электронная информационно-образовательная среда, система электронного документооборота) подлежат регулярному резервному копированию с хранением не менее двух копий, включая копию на обособленном (в том числе облачном отечественном) ресурсе.

5.6. Информационно-телекоммуникационная сеть Университета подлежит логическому разделению на сегменты в зависимости от категории обрабатываемой информации (сегмент бухгалтерии, сегмент административного персонала, сегмент работы с государственными информационными системами, гостевой сегмент), в соответствии с мерами, предусмотренными Приказом ФСТЭК России № 21 и Приказом ФСТЭК России № 117.

5.7. Университет обеспечивает предотвращение утечек информации ограниченного доступа с применением организационных и технических мер. Порядок применения средств

контроля устанавливается отдельными локальными нормативными актами Университета с соблюдением законодательства Российской Федерации.

5.8. Использование сети «Интернет» и электронной почты в служебных целях осуществляется в соответствии с должностными обязанностями работников. Использование ресурсов Университета в личных целях, способных повлечь угрозу информационной безопасности, не допускается.

6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Университет обеспечивает своевременное выявление, регистрацию, анализ и устранение последствий инцидентов информационной безопасности, а также информирование уполномоченных государственных органов в случаях, предусмотренных законодательством Российской Федерации.

6.2. Порядок информирования, реагирования, расследования инцидентов и взаимодействия ответственных должностных лиц определяется Регламентом реагирования на инциденты информационной безопасности Университета.

7. ОТВЕТСТВЕННОСТЬ

7.1. Работники, нарушившие требования настоящей Политики и иных локальных актов в области информационной безопасности, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

8. ПЕРЕСМОТР ПОЛИТИКИ

8.1. Настоящая Политика подлежит пересмотру не реже одного раза в три года, а также при существенном изменении законодательства Российской Федерации в области информационной безопасности, структуры информационных систем Университета или организационной структуры Университета.

8.2. Политика вступает в силу с даты утверждения ректором Университета и действует до утверждения новой редакции.

Лист ознакомления с Политикой информационной безопасности

№	Ф.И.О., должность	Дата ознакомления	Подпись
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			