	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
	Регламент организации работы с персональными данными в структурных подразделениях и служебных помещениях 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.

РЕГЛАМЕНТ РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ И ИНЦИДЕНТЫ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «АРМАВИРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Р-1-30-10-26

Армавир, 2026 г.

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	*№ 31 от «23» октября 2026г.*
Р-1-30-10-26	Стр. 1 из 10

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент устанавливает порядок обнаружения, фиксации, расследования компьютерных инцидентов и инцидентов, связанных с обработкой персональных данных, а также порядок уведомления уполномоченных органов в федеральном государственном бюджетном образовательном учреждении высшего образования «Армавирский государственный педагогический университет» (далее — Университет).

1.2. Регламент разработан с учётом Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных» (включая часть 3.1 статьи 21), применимых требований Федерального закона от 26.07.2017 № 187-ФЗ и приказа ФСБ России от 25.12.2025 № 547. Регламент применяется во взаимосвязи с Политикой информационной безопасности, Положением об обработке и защите персональных данных (документом, определяющим политику Университета в отношении обработки персональных данных) и приказом о распределении обязанностей Университета. Применение требований законодательства не означает признания конкретных информационных систем Университета объектами критической информационной инфраструктуры без соответствующих правовых оснований.

1.3. Действие Регламента распространяется на все структурные подразделения и всех работников Университета.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Компьютерный инцидент — факт нарушения и (или) прекращения функционирования информационной системы, информационно-телекоммуникационной сети или иного информационного ресурса Университета и (или) нарушения безопасности обрабатываемой ими информации, в том числе произошедший в результате компьютерной атаки.

Инцидент, связанный с обработкой персональных данных — неправомерная или случайная передача (предоставление, распространение, доступ), повлёкшая нарушение прав субъектов персональных данных.

НКЦКИ — Национальный координационный центр по компьютерным инцидентам.

3. КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ

Тип	Примеры	Кому уведомлять
Компьютерный инцидент на информационных системах и	DDoS-атака, несанкционированный доступ к серверам, шифровальщик, нарушение работы сети или информационных систем Университета	НКЦКИ — в порядке и сроки приказа ФСБ № 547; учредитель — п. 7.4

Тип	Примеры	Кому уведомлять
ресурсах Университета		
Инцидент с ПДн	Утечка, несанкционированный доступ, утрата носителя с ПДн, компрометация учётной записи с доступом к ИСПДн	Роскомнадзор — 24 / 72 часа; учредитель — п. 7.4
Внутренний ИТ-инцидент	Сбой оборудования, вирусное заражение без утечки данных, нарушение работоспособности сервиса	Внутренняя регистрация и оценка; необходимость внешнего уведомления определяется характером события и применимыми требованиями.
Компрометация ключа ЭП / СКЗИ	Утрата токена, подозрение на использование ключа третьим лицом	Незамедлительно уведомить внутренние ответственные службы и удостоверяющий центр в предусмотренных случаях; отзыв сертификата — по установленной процедуре.

4. ПОРЯДОК ОБНАРУЖЕНИЯ И ФИКСАЦИИ ИНЦИДЕНТА

4.1. Любой работник, выявивший признаки инцидента, незамедлительно, но не позднее одного часа сообщает главному специалисту по защите информации и начальнику отдела безопасности доступным защищённым способом. При непосредственной угрозе работе системы одновременно информируется техническая служба (отдел информационной политики) для принятия неотложных мер.

4.2. Начальник отдела безопасности организует регистрацию сообщения в карточке учёта инцидента (приложение № 1), первичную оценку, назначение исполнителей и принятие мер реагирования. Главный специалист по защите информации осуществляет профильный контроль полноты документирования инцидента и соблюдения установленных требований и сроков в пределах предоставленных полномочий, не подменяя технических исполнителей.

4.3. Начальник отдела безопасности совместно с техническими специалистами определяет тип, масштаб и затронутые информационные ресурсы, признаки нарушения безопасности персональных данных и необходимость внешних уведомлений. Технические специалисты документируют исходные фактические сведения и передают их начальнику отдела безопасности; главному специалисту по защите информации предоставляются копии материалов для подготовки проектов уведомлений и профильного контроля.

5. ПОРЯДОК УВЕДОМЛЕНИЯ НКЦКИ (ИНЦИДЕНТЫ НА ИНФОРМАЦИОННЫХ СИСТЕМАХ И РЕСУРСАХ УНИВЕРСИТЕТА)

5.1. При выявлении компьютерного инцидента, подлежащего информированию НКЦКИ, начальник отдела безопасности организует сбор и проверку исходных сведений от эксплуатирующих и иных структурных подразделений. Главный специалист по защите информации на основании переданных документально зафиксированных сведений готовит проект сообщения НКЦКИ и передаёт его на согласование проректору по безопасности (либо уполномоченному замещающему лицу). Официальное направление осуществляет уполномоченное должностное лицо Университета в порядке и сроки, предусмотренные приказом ФСБ России от 25.12.2025 № 547. Согласование организуется без нарушения обязательных сроков; при отсутствии руководителя применяется установленный Университетом порядок замещения.

5.2. Состав, формат, каналы передачи первоначальных и уточняющих сведений, а также сроки взаимодействия с НКЦКИ определяются применимыми требованиями приказа ФСБ России № 547. Отправитель документирует дату, время, канал и подтверждение передачи сообщения; эти сведения включаются в карточку инцидента. Внутренний шаблон (приложение № 2) используется лишь как рабочая форма сбора сведений и не заменяет обязательные форматы сообщений.

6. ПОРЯДОК УВЕДОМЛЕНИЯ РОСКОМНАДЗОРА (ИНЦИДЕНТЫ С ПДН)

6.1. При установлении факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлёкшей нарушение прав субъектов персональных данных, Университет уведомляет Роскомнадзор в соответствии с частью 3.1 статьи 21 Федерального закона № 152-ФЗ: в течение 24 часов с момента выявления инцидента — об инциденте, его предполагаемых причинах и последствиях, предполагаемом вреде и принятых мерах; в течение 72 часов с момента выявления — о результатах внутреннего расследования и лицах, действия которых стали причиной инцидента (при наличии). Начальник отдела безопасности организует сбор и проверку исходных сведений и проведение расследования. Главный специалист по защите информации готовит проекты уведомлений на основании документально зафиксированных материалов, передаёт их проректору по

безопасности на согласование; направление обеспечивает уполномоченное должностное лицо Университета без нарушения установленных сроков.

6.2. При отсутствии полного объёма подтверждённых сведений к моменту направления первичного уведомления указываются имеющиеся сведения с обозначением их предварительного характера; сбор и уточнение информации продолжаются. Отсутствие согласующего руководителя не является основанием для пропуска установленного законом срока: применяется предусмотренный приказом порядок замещения.

6.3. Дата и время выявления инцидента, представления исходных сведений, согласования и направления уведомлений, а также подтверждения их приёма фиксируются в карточке инцидента. Рабочий шаблон приложения № 3 не заменяет утверждённые формы и официальные способы подачи сведений Роскомнадзору.

6.4. Правовое основание уведомления Роскомнадзора — часть 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ.

7. РАССЛЕДОВАНИЕ И ЗАКРЫТИЕ ИНЦИДЕНТА

7.1. Начальник отдела безопасности организует внутреннее расследование с участием технических специалистов и соответствующих подразделений. Исполнители фиксируют обстоятельства, технические факты, причины, последствия, доказательства и принятые меры в материалах расследования. Главный специалист по защите информации анализирует представленные материалы, осуществляет профильный контроль и готовит предложения по предупреждению повторных инцидентов в пределах полномочий.

7.2. Решение о закрытии инцидента принимается начальником отдела безопасности после подтверждения устранения последствий, документирования расследования и направления необходимых уведомлений; в случае существенных последствий — по согласованию с проректором по безопасности. Главный специалист по защите информации проверяет полноту материалов и выполнение контрольных мероприятий.

7.3. Материалы расследования хранятся в деле информационной безопасности не менее 5 (пяти) лет.

7.4. При наличии обязанности информировать учредителя по установленным требованиям или указаниям Министерства просвещения Российской Федерации начальник отдела безопасности организует подготовку проекта сообщения на основании материалов расследования. Главный специалист по защите информации может готовить текст проекта по документально подтверждённым сведениям. Сообщение согласовывается с проректором по безопасности и направляется ректором либо уполномоченным им лицом в установленном учредителем порядке и сроки. Если специальная форма не установлена, допускается использовать рабочий образец из приложения № 4. Самостоятельный универсальный срок информирования учредителя настоящим Регламентом не вводится.

7.5. Информирование учредителя не заменяет и не откладывает уведомление НКЦКИ и Роскомнадзора. Персональные данные субъектов в сообщение учредителю не включаются.

8. ОТВЕТСТВЕННОСТЬ

8.1. За нарушение настоящего Регламента работники могут привлекаться к ответственности при наличии предусмотренных законом оснований и с соблюдением установленного порядка, в том числе статей 192–193 Трудового кодекса Российской Федерации. Установление нарушения, вины и обстоятельств его совершения осуществляется в предусмотренном законодательством порядке.

8.2. Проректор по безопасности осуществляет общее руководство организацией реагирования на инциденты и согласование проектов уведомлений в пределах полномочий. Начальник отдела безопасности организует расследование инцидентов, сбор материалов и обеспечивает своевременную подготовку обязательных уведомлений. Технические и иные структурные подразделения своевременно предоставляют полные и достоверные исходные сведения и исполняют порученные мероприятия. Главный специалист по защите информации готовит проекты уведомлений на основании представленных материалов и осуществляет профильный контроль в пределах полномочий. Ответственность работников определяется их должностными обязанностями и законодательством Российской Федерации.

Приложение № 1 к Регламенту реагирования на компьютерные инциденты

КАРТОЧКА УЧЁТА ИНЦИДЕНТА № _____

Дата и время обнаружения	
Кто обнаружил (ФИО, должность)	
Тип инцидента	☐ Компьютерный ☐ ПДн ☐ Внутренний ИТ ☐ Компрометация ЭП/СКЗИ
Затронутая информационная система	
Краткое описание инцидента	
Предполагаемая причина	
Объём затронутых данных / субъектов	
Принятые первичные меры	
Необходимость уведомления НКЦКИ	☐ Да, направлено ____.____.20___ в ____:____ ☐ Не требуется
Необходимость уведомления РКН (24ч)	☐ Да, направлено ____.____.20___ в ____:____ ☐ Не требуется
Уведомление РКН (72ч, расследование)	☐ Да, направлено ____.____.20___ в ____:____ ☐ Не требуется
Информирование учредителя (Минпросвещения России)	☐ Да, направлено ____.____.20___ в ____:____ ☐ Не требуется
Ответственный за расследование	
Дата закрытия инцидента	
Итоговые меры / выводы	

Приложение № 2 к Регламенту реагирования на компьютерные инциденты

ШАБЛОН УВЕДОМЛЕНИЯ НКЦКИ О КОМПЬЮТЕРНОМ ИНЦИДЕНТЕ

(рабочая форма для сбора информации; обязательные каналы и форматы взаимодействия устанавливаются приказом ФСБ России № 547)

Наименование организации: федеральное государственное бюджетное образовательное учреждение высшего образования «Армавирский государственный педагогический университет»

ИНН: 2302022685

Наименование информационной системы (ресурса), на которой произошёл инцидент: _____

Дата и время обнаружения инцидента: ____.____.20___ г., ____:____

Описание инцидента: _____

Предполагаемые причины: _____

Предполагаемый вред: _____

Принятые меры по устранению последствий: _____

Контактное лицо, уполномоченное Университетом для взаимодействия: ФИО _____, должность _____, телефон _____, e-mail _____

Дата составления: ____.____.20___ г.

Приложение № 3 к Регламенту реагирования на компьютерные инциденты

ШАБЛОН ПЕРВИЧНОГО УВЕДОМЛЕНИЯ РОСКОМНАДЗОРА ОБ ИНЦИДЕНТЕ, СВЯЗАННОМ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

(рабочая форма; уведомление направляется по установленной Роскомнадзором форме и каналу в сроки, предусмотренные частью 3.1 статьи 21 Федерального закона № 152-ФЗ)

Наименование оператора: ФГБОУ ВО «АГПУ», ИНН 2302022685

Дата и время обнаружения инцидента: ____.____.20___ г., ____:____

Описание произошедшего: _____

Предполагаемые причины: _____

Категории и примерное количество затронутых субъектов ПДн: _____

Предполагаемый вред, причинённый субъектам ПДн: _____

Принятые меры по устранению последствий: _____

Уполномоченное лицо для направления уведомления: должность, ФИО _____

Примечание: в течение 72 часов с момента обнаружения необходимо направить дополнительное уведомление с результатами внутреннего расследования.

Приложение № 4 к Регламенту реагирования на компьютерные инциденты

ШАБЛОН ИНФОРМАЦИОННОГО СООБЩЕНИЯ УЧРЕДИТЕЛЮ О КОМПЬЮТЕРНОМ ИНЦИДЕНТЕ ИЛИ ИНЦИДЕНТЕ, СВЯЗАННОМ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

(направляется учредителю — Министерству просвещения Российской Федерации — в порядке, установленном учредителем; применяется, если учредителем не установлена иная форма)

Наименование организации: ФГБОУ ВО «АГПУ», ИНН 2302022685

Дата и время обнаружения инцидента: ____.____.20___ г., ____:____

Тип инцидента: ☐ компьютерный инцидент ☐ инцидент, связанный с обработкой ПДн ☐ иное: _____

Затронутая информационная система (ресурс): _____

Краткое описание инцидента: _____

Категории затронутых данных и примерное количество субъектов (без указания самих персональных данных): _____

Принятые меры по устранению последствий: _____

Направлены уведомления: ☐ НКЦКИ ____.____.20___ ☐ Роскомнадзор ____.____.20___ ☐ не требуются

Составитель проекта / уполномоченный отправитель: должность, ФИО _____; телефон _____, e-mail _____

Примечание: информирование учредителя не заменяет и не откладывает уведомление НКЦКИ и Роскомнадзора. Персональные данные в сообщение не включаются.