**УТВЕРЖДАЮ:**

 **Ректор ФГБОУ ВО «СевКавГА»**

 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Р.М. Кочкаров/**

 **« \_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2025 г.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
| **ПОЛОЖЕНИЕ** | **ИНСТРУКЦИЯ** |
| **о порядке организации и проведении работ по защите персональных данных, обрабатываемых в информационных системах персональных данных в ФГБОУ ВО «Северо-Кавказская государственная академия»** | **ответственного пользователя средств криптографической защиты информации в ФГБОУ ВО «Северо-Кавказская государственная академия»** |

 |
|  |

**Черкесск, 2025**

# Общие положения

* 1. Настоящее Положение о порядке организации и проведении работ по защите персональных данных, обрабатываемых в информационных системах персональных данных в ФГБОУ ВО «Северо-Кавказская государственная академия» (далее – Положение) разработано в соответствии со следующими нормативными правовыми актами Российской Федерации в области обработки и защиты персональных данных:
* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
* приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
	1. Сокращения, термины и определения

В настоящем Положении используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

| **Сокращение** | **Расшифровка сокращения** |
| --- | --- |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю |
| Антивирусное ПО | Программное обеспечение средств антивирусной защиты |
| Вредоносное ПО | Вредоносная компьютерная программа (вирус) |
| АРМ | Автоматизированное рабочее место |
| ПДн | Персональные данные |
| ПО | Программное обеспечение |
| СВТ | Средства вычислительной техники |

Таблица 2 – Перечень терминов и определений

| **Термин** | **Определение** | **Источник** |
| --- | --- | --- |
| Администратор безопасности информационной системы персональных данных (администратор безопасности) | Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных |  |
| Администратор системный | Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) в соответствии с установленной ролью |  |
| Вредоносная программа | Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы | ГОСТ Р 51275-2006 |
| Информационная система | Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств | ГОСТ Р 51583-2014 |
| Инцидент информационной безопасности | Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность | ГОСТ Р ИСО МЭК 27001 |
|  (компьютерный) вирус | Вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы |  ГОСТ Р 51275-2006 |
| Машинный носитель информации | Материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе персональных данных (далее – ПДн)) в электронном виде. |  |
| Персональные данные | Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) | Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» |
| Событие информационной безопасности | Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью | ГОСТ Р ИСО МЭК 27001 |

* 1. Администратор безопасности, администратор системный и пользователи информационных систем персональных данных (далее – информационных систем) должны быть ознакомлены с настоящей Инструкцией до начала работы в информационных системах под подпись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.
	2. Для координации и контроля выполнения мероприятий по организации обработки и защиты персональных данных в ФГБОУ ВО «Северо-Кавказская государственная академия» назначается лицо, ответственное за организацию обработки персональных данных.

При выполнении своих служебных (трудовых) обязанностей ответственный за организацию обработки персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия» руководствуется требованиями Инструкции ответственного за организацию обработки персональных данных ФГБОУ ВО Северо-Кавказская государственная академия».

* 1. В ФГБОУ ВО Северо-Кавказская государственная академия» утверждены Правила обработки персональных данных информационных систем персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия» в целях:
* обеспечения защиты прав и свобод субъектов персональных данных при обработке персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия»;
* установления процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации о персональных данных, иных правовых актов Российской Федерации, внутренних документов ФГБОУ ВО Северо-Кавказская государственная академия» по вопросам обработки и защиты персональных данных;
* определения целей обработки персональных данных в информационных системах в установленной сфере деятельности, включая содержание обрабатываемых персональных данных, категории субъектов персональных данных, данные которых обрабатываются, сроки обработки (в том числе хранения) обрабатываемых персональных данных, а также порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований;
* установления ответственности работников ФГБОУ ВО Северо-Кавказская государственная академия», имеющих доступ к персональным данным субъектов персональных данных в информационных системах, за невыполнение требований норм, регулирующих обработку персональных данных, установленных законодательством Российской Федерации, настоящим Положением и иными локальными актами ФГБОУ ВО Северо-Кавказская государственная академия».
	1. Для непосредственного выполнения работ по защите персональных данных с использованием программно-аппаратных средств защиты информации назначается лицо, ответственное за обеспечение безопасности персональных данных в информационных системах (далее – администратор безопасности)

При выполнении своих обязанностей администратор безопасности действует в соответствии с требованиями Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия» и требованиями эксплуатационной документации на средства защиты информации, используемые в составе системы защиты информации.

* 1. Все пользователи информационных систем участвуют в защите персональных данных, содержащейся в информационных системах, и обязаны знать и выполнять требования:
* нормативных правовых документов Российской Федерации по защите информации, в том числе по защите персональных данных;
* настоящего Положения и перечисленных в нём инструкций, в части их касающейся;
* Инструкции пользователя информационных систем персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	1. В ходе эксплуатации информационных систем персональных данных защита персональных данных обеспечивается выполнением процедур:
* управления (администрирования) системой защиты информации в информационных системах;
* контроля обеспечения уровня защищённости персональных данных в информационных системах.

# Управление системой защиты персональных данных информационных систем

* 1. Процедуры управления системой защиты персональных данных обеспечивают:
	+ функционирование системы защиты персональных данных информационных систем в штатном режиме с характеристиками, установленными в проектной документации;
	+ документированный поток информации о событиях безопасности в информационных системах и их системах защиты, на основании которой возможны реализация процедуры контроля уровня защищённости персональных данных, обрабатываемых в информационных системах.
	1. Порядок действий пользователей информационных систем при прохождении процедур идентификации (узнавании) и аутентификации (подтверждении подлинности узнанного пользователя) при входе в информационные системы описаны в Инструкции по идентификации и аутентификации пользователей информационных систем персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	2. Порядок управления доступом пользователей к информационным ресурсам информационных систем устанавливается в Инструкции по управлению доступом к информационным системам персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	3. Порядок действий пользователей информационных систем при работе с машинными носителями персональных данных, правила учёта, хранения и доступа к машинным носителям описаны в Инструкции по защите машинных носителей персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	4. Порядок действий администратора безопасности и системных администраторов информационных систем при появлении событий безопасности описаны в Инструкции по управлению событиями информационной безопасности информационных систем персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	5. Порядок действий пользователей при обнаружении вредоносного ПО, описаны в Инструкции по антивирусной защите информационных систем персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	6. Порядок действий системных администраторов и администратора безопасности информационных систем с целью:
	+ выявления ошибок и недостатков программного обеспечения и аппаратных средств, и средств защиты персональных данных информационных систем;
	+ контроля установки обновлений программного обеспечения, контроля работоспособности и настроек программного обеспечения;
	+ контроля состава технических и программных средств информационных систем, в том числе средств защиты информации, описан в Инструкция по контролю (анализу) защищенности персональных данных информационных систем персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	1. Порядок доступа пользователей к техническим средствам информационных систем, в том числе к техническим средствам системы защиты информации описан в Инструкции по защите технических средств информационных систем персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	2. Организация резервного копирования и восстановления персональных данных в информационных системах осуществляется администратором безопасности с заданной периодичностью, определяемой Инструкцией по обеспечению доступности информации информационных систем персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия» (при наличии).
	3. Организация режима безопасности помещений, в которых размещены информационные системы, правила доступа в помещения в рабочее, нерабочее время и в нештатных ситуациях определены в Порядке доступа в помещения, в которых размещены информационные системы персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия».
	4. Обеспечение безопасности персональных данных, при обработке в информационных системах с использованием средств криптографической защиты информации, осуществляется в соответствии с Положением по использованию средств криптографической защиты информации в ФГБОУ ВО Северо-Кавказская государственная академия», Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в ФГБОУ ВО Северо-Кавказская государственная академия», Инструкцией пользователя средств криптографической защиты информации в ФГБОУ ВО Северо-Кавказская государственная академия», Инструкцией ответственного пользователя средств криптографической защиты информации в ФГБОУ ВО Северо-Кавказская государственная академия».
1. **Контроль обеспечения уровня защищённости персональных данных информационных систем**
	1. Периодичность контроля обеспечения уровня защищённости персональных данных, обрабатываемых в информационных системах, составляет 1 год.
	2. Для контроля обеспечения уровня защищённости используются следующие документы:
	* отчёты о событиях информационной безопасности;
	* результаты контроля защищённости;
	* информация из специальных источников по новым угрозам безопасности для используемых в информационных системах программных и программно – технических средств.
	1. На основе указанных выше документов, ответственный за организацию обработки персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия»:
* анализ функционирования системы защиты информации, включая сбои и неисправности аппаратно-программных средств защиты информации;
* анализ изменения угроз безопасности персональных данных, обрабатываемых в информационных системах.
	1. К анализу привлекаются системные администраторы и администратор безопасности. По отдельному договору к анализу могут быть привлечены специалисты сторонних организаций.
	2. Ответственный за организацию обработки персональных данных в ФГБОУ ВО Северо-Кавказская государственная академия» организует документирование результатов проведённого анализа в виде Акта контроля обеспечения защищённости персональных данных (акт составляется в произвольной форме и подписывается ответственным за организацию обработки ПДн в ФГБОУ ВО Северо-Кавказская государственная академия» и администратором безопасности).
	3. На основании выводов Акта контроля защищённости персональных данных ответственный за организацию обработки персональных данных ФГБОУ ВО Северо-Кавказская государственная академия» при необходимости доработки системы защиты персональных данных докладывает об этом руководителю ФГБОУ ВО Северо-Кавказская государственная академия». Решение о доработке и последующей аттестации принимает руководитель ФГБОУ ВО Северо-Кавказская государственная академия».
1. **Ответственность**
	1. Пользователи информационных систем должны быть предупреждены об ответственности за действия персональными данными, содержащимися в информационных системах, и действия с техническими средствами информационных систем, и системы защиты информации, нарушающие требования настоящего Положения и других организационно-распорядительных документов, определяющих меры по защите персональных данных в информационных системах.

Разработано:

Начальник УК О. П. Фетисова

Согласовано:

И.о.начальника ПУ А.Б. Тохчукова