

Приложение № 16
к приказу АНО ДО «Парк «Патриот»
им. Героя РФ Серафимова М.В.»
от 13.05.2026 г. № 135

Рассмотрено на общем собрании
работников АНО ДО «Парк «Патриот»
им. Героя РФ Серафимова М.В.»
(протокол от 27.10.2025 г. № 1)

Утверждено Советом АНО ДО «Парк
«Патриот» им. Героя РФ Серафимова М.В.»
(протокол от 22.04.2026 г.)

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных в Автономной
некоммерческой организации дополнительного образования «Военно-
патриотический парк Республики Башкортостан «Патриот» имени Героя
Российской Федерации Серафимова Максима Владимировича»

1. Общие положения

1.1 Инструкция пользователя информационных систем персональных данных в АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.» (далее – Инструкция) определяет в АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.» обязанности, права и ответственность пользователей информационных систем персональных данных (далее – информационные системы).

1.2 Пользователями информационных систем являются работники АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.», допущенные к обработке персональных данных в информационных системах в соответствии с утвержденным в АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.» перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационных системах персональных в АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.» необходим для выполнения ими трудовых (служебных) обязанностей.

1.3 Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
АРМ	Автоматизированное рабочее место
ПДн	Персональные данные
СВТ	Средства вычислительной техники
ПО	Программное обеспечение

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	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде.	
Машинный носитель персональных данных	Машинный носитель информации, на которых хранятся и (или) обрабатываются персональные данные	
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»

1.4 Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- 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 ФСБ России от 10.07.2014 № 378 Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требованиям к защите персональных данных для каждого из уровней защищенности»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.5 Пользователи информационных систем должны быть ознакомлены с настоящей Инструкцией до начала работы в информационных системах. Обязанность

по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Обязанности пользователей информационных систем

2.1. Пользователи информационных систем обязаны знать и выполнять требования законодательства Российской Федерации и локальных актов АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.», устанавливающих правила обработки и защиты ПДн в информационных системах.

2.2. При эксплуатации информационных систем с целью защиты ПДн пользователь обязан:

- руководствоваться требованиями организационно-распорядительной документации по организации обработки и защиты персональных данных;
- соблюдать установленную технологию обработки и защиты ПДн;
- знать свои идентификаторы и пароли, осуществлять ввод паролей в условиях, исключающих их просмотр;
- не записывать значения паролей на бумагу, электронные носители, иные предметы и не разглашать (не сообщать или любым другим способом не доводить до кого либо, включая работников АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.», в т.ч. руководителей, администратора безопасности и системного администратора, значения действующих паролей;
- осуществлять смену пароля не реже, чем через 90 дней;
- ежедневно вести антивирусный контроль на непосредственных средствах вычислительной техники (далее – СВТ);
- проверять вложения электронной почты, съемные машинные носители информации перед началом работы на предмет наличия вредоносного программного обеспечения;
- использовать для записи ПДн только съемные машинные носители информации, учтенные в установленном порядке;
- хранить съемные машинные носители персональных данных в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним;
- использовать для вывода на печать документов, содержащих информацию, находящуюся в информационных системах, только устройства печати, расположенные в пределах установленных контролируемых зон, сводя к минимуму возможность доступа к ним посторонних лиц.

2.3. Пользователь должен свести к минимуму возможность неконтролируемого доступа к средствам вычислительной техники (далее - СВТ) информационных систем посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на СВТ работ.

В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются СВТ информационных систем, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить СВТ.

Защищаемые носители информации должны быть убраны в запираемые хранилища, определенные в установленном порядке для этих целей.

2.4. Докладывать администратору безопасности и своему непосредственному руководителю (при наличии):

- о фактах имевшегося или предполагаемого несанкционированного доступа к информации, носителям информации, СВТ информационных систем, помещениям, в которых располагаются СВТ информационных систем, и хранилищам;
- об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка ПДн и хранилищ;
- об обнаружении вредоносного ПО (сообщение на экране монитора о наличии вируса), и иных предупреждающих сообщений средств антивирусной защиты (истечения срока лицензии, о неактуальности базы данных, о наличии признаков вредоносных компьютерных программ (вирусов) и т.п.), а также при нетипичном поведении СВТ информационных систем (медленная работа при открытии приложений, частое зависание ПО, самопроизвольный перезапуск, сбой в работе);
- о попытках получения информации лицами, не имеющими к ней допуска;
- о попытках неконтролируемого проникновения посторонних лиц в помещения контролируемой зоны информационных систем;
- об иных внештатных ситуациях, связанных с угрозой безопасности информационных систем.

2.5. Пользователю запрещается:

- подключать к СВТ информационных систем нештатные устройства;
- применять в информационных системах незарегистрированные машинные носители информации либо использовать учтенные машинные носители информации в неслужебных целях;
- выносить машинные носители информации, мобильные технические средства данных за пределы контролируемой зоны АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.» без письменного разрешения руководителя;
- несанкционированно вносить незарегистрированные машинные носители информации, мобильные технические средства;
- блокировать, изменять настройки и выгружать антивирусное ПО на своих СВТ;
- самостоятельно осуществлять подключение (отключение) СВТ к локальной вычислительной сети;
- продолжать работы на СВТ при обнаружении вредоносного ПО в процессе обработки информации;
- самостоятельно вносить изменения в состав, конфигурацию и размещение СВТ информационных систем;
- самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в информационных системах;
- самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (далее – СЗИ) информационных систем;
- сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от хранилищ и помещений и другие реквизиты доступа к информационным системам;
- разрешать работу с СВТ информационных систем лицам, не допущенным к обработке ПДн в установленном порядке;
- находиться в нерабочее время в помещениях, где размещено оборудование информационных систем и СЗИ без служебной записки (или иного вида разрешающего документа), подписанного генеральным директором АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.».

3. Права пользователей информационных систем

3.1. Пользователь информационных систем имеет право:

- обращаться к администратору безопасности, системному администратору информационных систем и ответственному за организацию обработки ПДн по любым вопросам, касающимся обработки и защиты информации в информационных системах (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации информационных систем);
- обращаться к администратору безопасности с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в информационных системах информации, а также по вопросам эксплуатации установленных средств защиты информации (СЗИ);
- обращаться к системному администратору информационных систем и администратору безопасности с просьбой об оказании консультаций и технической помощи по использованию установленных программных и технических средств информационных систем.

4. Ответственность

4.1. На пользователя информационных систем возлагается персональная ответственность:

- за соблюдение установленной технологии обработки ПДн;
- за соблюдение режима конфиденциальности информации;
- за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в информационных системах;
- за соблюдение требований локальных актов по вопросам обработки и защиты ПДн в информационных системах.

4.2. Работники АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.» несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.