

Приложение № 13
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 № 1 от 27.10.2025 г.)

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

ИНСТРУКЦИЯ
по контролю (анализу) защищенности персональных данных
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. Настоящая Инструкция по контролю (анализу) защищенности персональных данных информационных систем 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.» порядок выявления (поиска), анализа и устранения уязвимостей информационных систем персональных данных (далее – информационные системы), недостатков программного обеспечения, аппаратных средств, организационно-технических недостатков, а также порядок действий администратора безопасности и системных администраторов информационных систем при контроле защищенности персональных данных, обрабатываемых в информационных системах.

1.2. Сокращения, термины, определения

В настоящей Инструкции 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
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средства защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	

Термин	Определение	Источник
(администратор безопасности)		
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
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»
Уязвимость	Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации	ГОСТ Р 56545-2015
Уязвимость информационной системы	Свойство информационной системы, предоставляющее возможность реализации угроз безопасности обрабатываемой в ней информации	ГОСТ Р 50922-2006

1.3. 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 ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Пользователи 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 в АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.».

2. Выявление анализ и устранение уязвимостей информационных систем

2.1. С целью предотвращения реализации угроз безопасности осуществляется выявление (поиск), анализ и устранение уязвимостей информационных систем.

2.2. Периодичность плановых процедур выявления, анализа и устранения уязвимостей информационных систем составляет не реже одного раза в год.

Внеплановые процедуры выявления, анализа и устранения уязвимостей информационных систем проводят по распоряжению ответственного за организацию обработки ПДн в случае необходимости. Необходимость внеплановой процедуры

выявления и устранения уязвимостей определяет ответственный за организацию обработки ПДн на основе анализа журналов событий безопасности.

2.3. В информационных системах должно осуществляться выявление и устранение следующих типов уязвимостей:

- недостатки и (или) ошибки кода в ПО (общесистемном, прикладном, специальном) информационных систем и ПО ее системы защиты информации;
- недостатки аппаратных средств информационных систем, в том числе аппаратных средств защиты информации;
- организационно-технические недостатки.

2.4. Мероприятия по выявлению, анализу и устранению уязвимостей организует ответственный за организацию обработки ПДн.

План устранения выявленных уязвимостей разрабатывает администратор безопасности.

Непосредственными исполнителями мероприятий по выявлению, анализу и устранению уязвимостей информационных систем являются администратор безопасности и системный администратор информационных систем в части касающейся.

2.5. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального ПО, технических средств, а также другие базы данных уязвимостей (опубликованные в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средств и ПО).

3. Недостатки программного обеспечения

3.1. Мероприятия по выявлению и анализу недостатков программного обеспечения информационных систем включают в себя выполнение следующих проверок:

- проверка конфигурации и настроек программно-технических средств информационных систем и системы защиты информации на соответствие требованиям эксплуатационной документации и требований к защите ПДн;
- проверка наличия и сроков действия лицензий на установленное программное обеспечение информационных систем;
- проверка наличия последних обновлений используемого программного обеспечения информационных систем и системы защиты информации;
- проверка соответствия обновлений версиям программного обеспечения, установленного в информационных системах и системе защиты информации;
- проверка обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты;
- проверка обновлений баз сигнатур уязвимостей средств контроля (анализа) защищенности (при использовании сканеров безопасности).

3.2. Проверочные мероприятия, указанные в пункте 3.1, и устранение обнаруженных недостатков на основании своих полномочий осуществляют администратор безопасности и системные администраторы информационных систем.

3.3. Все устанавливаемые обновления ПО информационных систем и ПО системы защиты информации должны быть предварительно проверены на работоспособность, а также на отсутствие вредоносного кода в соответствии с

Инструкцией по антивирусной защите информационных систем персональных данных в АНО ДО «Парк «Патриот» им. Героя РФ Серафимова М.В.».

3.4. После установки обновления программного обеспечения системный администратор и администратор безопасности каждый в своей части выполняют необходимые настройки, проводят тестирование работоспособности и вносят соответствующие изменения в эксплуатационную документацию (формуляр или паспорт) и Технические паспорта информационных систем.

3.5. Мониторинг наличия обновлений, выпускаемых разработчиками для всего используемого в информационных системах программного обеспечения, осуществляют не реже 1 раза в неделю администратор безопасности и системный администратор.

4. Недостатки аппаратных средств

4.1. К недостаткам аппаратных средств, используемых в информационных системах, относят низкую надежность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

4.2. При выявлении недостатков аппаратных средств проверяют:

- техническое состояние аппаратных средств, журналы планово-профилактического обслуживания аппаратных средств информационных систем за период контроля защищенности информационных систем;
- наличие сертификатов соответствия на примененные в информационных системах и их системах защиты информации аппаратные средства;
- наличие у поставщиков обновленных версий аппаратных средств, примененных в информационных системах и их системах защиты информации;
- перечень событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств;
- конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.

4.3. Проверочные мероприятия, указанные в пункте 4.2 настоящей Инструкции, осуществляет администратор безопасности с привлечением системного администратора.

5. Контроль установки обновлений программного обеспечения

5.1. Контроль установки обновлений ежеквартально проводит администратор безопасности.

5.2. Получение обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода осуществляется из доверенных источников.

5.3. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного обеспечения, включая программное обеспечение средств защиты информации, установленное в информационных системах и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке обновлений и в Технических паспортах информационных систем.

5.4. При обновлении программного обеспечения средств защиты информации аттестованной информационной системы – отправляется уведомление в орган по аттестации.

5.5. При контроле обновлений системы защиты информации осуществляется проверка версий:

- баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты;
- баз сигнатур уязвимостей средства контроля (анализа) защищенности (при использовании сканеров безопасности).

5.6. При получении информации о прекращении поддержки разработчиком используемого ПО в части выпуска обновлений безопасности, либо о планируемом прекращении такой поддержки администратор безопасности и системный администратор незамедлительно сообщают ответственному за организацию обработки ПДн.

6. Организационно-технические недостатки

6.1. Мероприятия по выявлению, анализу и устранению организационно-технических недостатков включают в себя выполнение следующих проверок:

- проверка состояния и актуальности организационно-распорядительной документации (далее – ОРД) по защите ПДн, обрабатываемых в информационных системах;
- проверка заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД);
- проверка соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям;
- проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям;
- проверка соответствия выполнения правил разграничения доступа к ПДн и ресурсам информационных систем принятым требованиям;
- проверка соответствия полномочий пользователей принятым требованиям;
- проверка наличия документов, подтверждающих правомерность изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;
- проверка состояния физической защиты информационных систем (средства охраны и физического доступа в контролируемых зонах информационных систем);
- проверка знания и соблюдения пользователями информационных систем основных нормативно-правовых актов в области защиты ПДн и требований ОРД;

6.2. Проверки организует ответственный за организацию обработки ПДн с участием администратора безопасности.

7. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

7.1. Администратором безопасности и системным администратором в части касающейся осуществляется периодический контроль конфигурации и настроек программно-технических средств информационных систем и средств защиты информации на соответствие требованиям эксплуатационной документации и требований к защите ПДн, в том числе:

- работоспособности (неотключения) ПО и средств защиты информации в информационных системах (ежедневно);

- правильности функционирования ПО и средств защиты информации в информационных системах (ежедневно);
- соответствия настроек ПО и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации в информационных системах (ежеквартально).

7.2. В случае выявления сбоев, отказов или несоответствия настройкам проводится восстановление ПО и СЗИ.

Восстановление производится с использованием резервных копий и (или) дистрибутивов.

7.3. Запрещается проводить обработку персональных данных в случае обнаружения неисправностей в системе защиты информации информационных систем.

8. Контроль состава технических средств, программного обеспечения и средств защиты информации

8.1. Контроль состава технических средств, ПО и средств защиты информации в информационных системах осуществляется с целью поддержания актуальной конфигурации программно-технических средств информационных систем.

8.2. Администратором безопасности не реже 1 раза в полгода проводится контроль на соответствие Техническому паспорту информационных систем состава технических средств, ПО и средств защиты информации.

8.3. Администратором безопасности не реже 1 раза в полгода проводится контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков.

9. Ответственность

9.1. 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.