Приложение №30

 утверждено приказом директора

 СОГБУ «демидовский КЦСОН»

 От\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_

**ИНСТРУКЦИЯ**

по организации анализа защищенности
информационных систем персональных данных в
смоленском областном государственном бюджетном учреждении

«Демидовский Комплексный Центр социального обслуживания населения»

# ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ разработан для реализации мер защиты информации, установленных в соответствии с требованиями приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также 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», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными документами по безопасности информации, и определяет порядок **контроля (анализа) защищенности информации** СОГБУ «Демидовский КЦСОН» (далее – учреждение), устанавливает ответственность администратора безопасности (АБИ).

* 1. Настоящий документ регламентирует правила и процедуры выявления, анализа и устранения уязвимостей в информационных системах учреждения и оперативное устранение вновь выявленных уязвимостей.
	2. К использованию в учреждении допускаются только сертифицированные ФСТЭК России средства **контроля (анализа) защищенности информации (САЗ)**, централизованно закупленные у разработчиков или поставщиков данных средств.
	3. Установка САЗ в учреждении осуществляется АБИ или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных САЗ и требованиями нормативных и методических документов ФСТЭК России.

# ПРИМЕНЕНИЕ СРЕДСТВ КОНТРОЛЯ (АНАЛИЗА) ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ (САЗ)

* 1. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.
	2. Меры по контролю (анализу) защищенности информации включают:

а) выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;

б) контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

в) контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

г) контроль состава технических средств, программного обеспечения и средств защиты информации;

д) контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

* 1. При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

а) выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

б) разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

в) анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

г) устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

д) информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

* 1. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.
	2. Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной оператором. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.
	3. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.
	4. АБИ должны организовать получение из доверенных источников (производителя САЗ) и установку обновлений базы признаков уязвимостей.

# ОСОБЕННОСТИ ОРГАНИЗАЦИИ АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ИОГВ

* 1. Анализ защищенности информационных систем учреждения в соответствии с требованиями настоящей Инструкции возлагается на специально назначенных администраторов безопасности информации (АБИ).
	2. Для анализа защищенности информационных систем учреждения АБИ используют сертифицированное средство анализа (контроля) защищенности (сканер безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.
	3. Перед проведением анализа защищенности информационных систем учреждения АБИ должен уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях.
	4. Доступ к функциям выявления (поиска) уязвимостей предоставляется только администраторам безопасности информации (АБИ).
	5. Периодичность проведения анализа защищенности информационных систем учреждения устанавливается приказом учреждения.