УТВЕРЖДАЮ
министр цифрового развития
и связи Кузбасса
_____ М.В. Садиков
«17» марта 2020 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
органам местного самоуправления и подведомственным учреждениям по осуществлению контроля защищенности информации в информационных системах

1. Общие положения

1.1. Настоящая инструкция регламентирует контроль уровня защищенности информации, обрабатываемой в информационных системах (далее – ИС) органов местного самоуправления Кемеровской области - Кузбасса (далее – ОМСУ), путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты информации.

2. Выявление, анализ и устранение уязвимостей информационной системы

2.1. В ИС ОМСУ при выявлении (поиске), анализе и устранении уязвимостей проводятся:

- 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;
- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- 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;
- информирование должностных лиц ОМСУ (пользователей, администраторов) о результатах поиска уязвимостей и оценки достаточности

реализованных мер защиты информации.

2.2. 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.

2.3. Выявление (поиск), анализ и устранение уязвимостей проводится на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится администраторами не реже одного раза в месяц. 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 ИС ОМСУ.

2.4. 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 (корректировка настроек средств защиты информации, изменение режима и порядка использования ИС ОМСУ), направленные на устранение возможности использования выявленных уязвимостей.

2.5. В ИС ОМСУ используются для выявления (поиска) уязвимостей средства анализа (контроля) защищенности (сканеры безопасности), имеющие 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, имеющие возможность оперативного обновления базы данных выявляемых уязвимостей.

2.6. В ИС ОМСУ осуществляется получение из доверенных источников и установка обновлений базы признаков уязвимостей (для системы анализа защищенности).

2.7. Доступ к функциям выявления (поиска) уязвимостей предоставляется только администратору информационной безопасности и администратору виртуальной инфраструктуры. Администратор информационной безопасности проводит анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в ИС ОМСУ для нарушения безопасности информации.

3. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации

3.1. В ИС ОМСУ администраторами в рамках своих полномочий осуществляется контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.2. В ИС ОМСУ администраторами в рамках своих полномочий осуществляется получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.3. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в ИС ОМСУ и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

3.4. Контроль установки обновлений проводится не реже одного раза в месяц.

3.5. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с Инструкцией по антивирусной защите в информационных ОМСУ, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

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

4.1. При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

- контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;
- контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в

эксплуатационной документации на систему защиты информации и средства защиты информации;

- восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

4.2. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится администраторами в рамках своих полномочий не реже одного раза в три месяца.

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

5.1. При контроле состава технических средств, программного обеспечения и средств защиты информации (инвентаризации) осуществляется:

- контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС ОМСУ и принятие мер, направленных на устранение выявленных недостатков;

- контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

- исключение (восстановление) из состава ИС ОМСУ несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5.2. Контроль состава технических средств, программного обеспечения и средств защиты информации проводится администраторами в рамках своих полномочий не реже одного раза в месяц.

6. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей, реализации правил разграничения доступа, полномочий пользователей в информационной системе

6.1. При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил

разграничения доступа, полномочий пользователей в ИС ОМСУ осуществляется:

- контроль правил генерации и смены паролей пользователей в соответствии с Правилами идентификации и аутентификации пользователей в ИС ОМСУ;

- контроль заведения и удаления учетных записей пользователей в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в ИС ОМСУ;

- контроль реализации правил разграничения доступа в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в ИС ОМСУ;

- контроль реализации полномочий пользователей в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах ОМСУ;

- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступа и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации в ОМСУ;

- устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

6.2. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИС ОМСУ проводится администратором информационной безопасности не реже одного раза в три месяца.

Начальник отдела данных
и информационной безопасности  С.С. Фомин