

УТВЕРЖДАЮ
Заместитель главы Администрации
города Ростова-на-Дону
по организационно-правовым
и кадровым вопросам

 А.Г. Новицкий
« 14 » февраля 2024 г.

ИНСТРУКЦИЯ
по выявлению (поиску), анализу и устранению уязвимостей на объектах
информатизации Администрации города Ростова-на-Дону

1. Общие положения

1.1. Инструкция по выявлению (поиску), анализу и устранению уязвимостей на объектах информатизации Администрации города Ростова-на-Дону, разработана в целях определения угроз безопасности информации, реализация которых может привести к нарушению системы защиты информации объектов информатизации (далее – ОИ), а также в целях предотвращения реализации данных угроз.

1.2. Проведение анализа уязвимостей ОИ позволяет оценить возможности преодоления нарушителем системы информационной безопасности ОИ и определить необходимые меры защиты.

1.3. На этапе эксплуатации ОИ поиск и анализ уязвимостей проводится по мере необходимости с учетом особенностей функционирования ОИ, но не реже одного раза в два года. 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 на ОИ.

1.4. Анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты ОИ в обязательном порядке проводится в ходе контроля за обеспечением уровня защищенности информации ОИ.

2. Порядок выявления (поиска), анализа и устранения уязвимостей на объектах информатизации Администрации города Ростова-на-Дону

2.1. Анализ уязвимостей ОИ включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения ОИ.

При анализе уязвимостей ОИ проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

В случае выявления уязвимостей ОИ, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем этих уязвимостей.

По результатам анализа уязвимостей должно быть подтверждено, что на ОИ отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

2.2. При выявлении (поиске), анализе и устранении уязвимостей на ОИ должно проводиться:

выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации;

формирование по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей;

определение мероприятий по устранению выявленных уязвимостей;

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 пользователей о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

2.3. 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, в том числе данные системы комплексного анализа защищенности Сканер-ВС.

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 (настройки средств защиты информации, изменение режима и порядка эксплуатации ОИ), направленные на устранение возможности использования выявленных уязвимостей.

Начальник управления
информационных технологий
Администрации города
Ростова-на-Дону



В.В. Егоренков