УТВЕРЖДЕН
приказом МБОУ СОШ
пос. Известковый
От 12.01.2024 № 05-Д

ПОРЯДОК
по анализу и установке обновлений безопасности программных, программно-аппаратных средств защиты информации и иного программного обеспечения в информационных системах муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы пос. Известковый

1.Данный документ определяет порядок и содержание работ по анализу и установке обновлений программного обеспечения, в том числе с открытым исходным кодом, предназначенного для устранения уязвимостей программных, программно-аппаратных средств (далее – обновления безопасности), применяемых в информационных системах муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы пос. Известковый (далее – ИС).

2.Устранение уязвимостей в сертифицированных программных, программно-аппаратных средствах защиты информации обеспечивается в приоритетном порядке и осуществляется в соответствии с эксплуатационной документацией на них, а также с рекомендациями разработчика.

3.Необходимость установки обновлений в целях устранения уязвимостей принимается с учетом особенностей функционирования уязвимой ИС (состав, масштаб, изолированность).

4.К анализу и тестированию принимаются преимущественно обновления, полученные доверенным способом. Источниками обновлений могут являться:

– официальные информационные ресурсы разработчиков программного обеспечения, программно-аппаратных средств и исследователей в области информационной безопасности;

– носители дистрибутивов;

– результаты тестирования обновлений программного обеспечения, содержащиеся в Банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

5.При анализе и тестировании обновлений необходимо руководствоваться методическим документом "Методика тестирования обновлений безопасности программных, программно-аппаратных средств", утвержденным ФСТЭК России 28 октября 2022 г. (далее – Методика тестирования).

6.К установке допускаются обновления безопасности, прошедшие процедуру тестирования на отсутствие потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации (далее – недекларированные

возможности). Источником информации об отсутствии недекларированных возможностей являются:

– результаты тестирования обновлений программного обеспечения, содержащиеся в Банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru);

– результаты самостоятельного тестирования, проведенного в соответствии с Методикой тестирования.