УТВЕРЖДАЮ
Приказ № 7-Д от «12» января 2024г
Директор МБОУ СОШ пос. Лесной
_____ О.Л.Кулак

ПОРЯДОК

по выявлению, анализу и устранению уязвимостей в информационных системах *Муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы пос. Лесной Амурского муниципального района Хабаровского края*

1. Данный документ регулирует порядок выявления, анализа и устранения уязвимостей в информационных системах *МБОУ СОШ пос. Лесной (далее - школа)*.

2. В качестве источника информации для выявления и устранения уязвимостей в ИС, а также определения уровня их критичности используются:

–отчет по результатам контроля защищенности ИС, проведенного отделом информационной безопасности, в том числе с использованием сканера уязвимостей;

–база уязвимостей программного обеспечения, программно-аппаратных средств, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также иные источники, содержащие сведения об известных уязвимостях;

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

– рекомендации, поступающие от Национального координационного центра по компьютерным инцидентам, Минцифры России, Управления ФСТЭК России по Дальневосточному федеральному округу.

Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют ИС.

3. В зависимости от уровня критичности уязвимостей программных, программно-аппаратных средств в ИС принимается решение о необходимости их устранения. Рекомендуемые сроки по устранению уязвимостей:

– 24 часа – для уязвимостей критического уровня;

– 7 дней – для уязвимостей высокого уровня;

– 30 дней – для уязвимостей среднего уровня;

–4 месяца – для уязвимостей низкого уровня.

4. Основным методом устранения уязвимостей является обновление программных, программно-аппаратных средств в соответствии с Порядком по анализу и установке обновлений безопасности программных, программно-аппаратных средств защиты информации и иного программного обеспечения в информационных системах *МБОУ СОШ пос. Лесной*, если иное не предусмотрено рекомендуемыми мерами.

5. В случае невозможности обновления программного обеспечения, программно-аппаратных средств с использованием официальных информационных ресурсов разработчиков программного обеспечения, программно-аппаратных средств, принимаются компенсирующие меры, в том числе с учетом рекомендаций, поступающих от Национального координационного центра по компьютерным инцидентам, Минцифры России, Управления ФСТЭК России по Дальневосточному федеральному округу. При реализации компенсирующих мер необходимо учитывать особенности функционирования ИС (состав, масштаб, изолированность).

6. Компенсирующими организационными и техническими мерами, направленными на предотвращение возможности эксплуатации уязвимостей, могут являться:

– изменение конфигурации уязвимых компонентов информационной системы, в том числе в части предоставления доступа к их функциям, исполнение которых может способствовать эксплуатации выявленных уязвимостей;

– ограничение по использованию уязвимых программных, программно-аппаратных средств или их перевод в режим функционирования, ограничивающий исполнение функций, обращение к которым связано с использованием выявленных уязвимостей (например, отключение уязвимых служб и сетевых протоколов);

– резервирование компонентов ИС, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;

– использование сигнатур, решающих правил средств защиты информации, обеспечивающих выявление в ИС признаков эксплуатации уязвимостей;

– мониторинг информационной безопасности и выявление событий безопасности информации в ИС, связанных с возможностью эксплуатации уязвимостей.