КОМИТЕТ ОБРАЗОВАНИЯ И НАУКИ АДМИНИСТРАЦИИ Г. НОВОКУЗНЕЦКА
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ НЕТИПОВОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
"Лицей №111"
654007, Россия, г.Новокузнецк, ул.Кирова 35, тел./факс 8(3843)46-82-08,
тел.46-05-33, 45-05-53,e-mail:litcey111@yandex.ru, http://www.liceym111.ru

СОГЛАСОВАНО
председатель профкома
_____ О.В. Митрохина
01.07.2021г.

Полюшко Марина Владимировна
Подписано цифровой подписью: Полюшко Марина Владимировна
Дата: 2021.09.20 13:03:41 +07'00'

УТВЕРЖДАЮ
директор МБ НОУ «Лицей № 111»
_____ М.В. Полюшко
01.07.2021г.

Инструкция № ИБ 12

по устранению уязвимостей программного обеспечения в информационной системе «МБ НОУ Лицей № 111»

1. Общие положения

1.1. Настоящая Инструкция по устранению уязвимостей программного обеспечения в информационной системе «**МБ НОУ Лицей № 111**» определяет правила и процедуры контроля (анализа) защищенности информации в информационной системе «**МБ НОУ Лицей № 111**» (далее – ИС), составленные с учетом требований приказа ФСТЭК России от 11.02.2013 № 17.

1.2. Анализ защищенности информации заключается в контроле установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

1.3. Ответственность за анализ защищенности информации ИС, а также за устранение уязвимостей программного обеспечения возлагается на системного администратора ИС.

1.4. Контроль отсутствия уязвимостей программного обеспечения ИС осуществляет администратор безопасности ИС путем проведения контрольных и выборочных проверок.

2. Порядок выполнения, анализа и устранения уязвимостей

2.1. В качестве инструментальных средств должны применяться сертифицированные по требованиям безопасности средства анализа защищенности.

2.2. Доступ к настройкам средств анализа защищенности должен быть предоставлен только администратору безопасности ИС (защищен паролем).

2.3. Анализ всех сетевых узлов ИС проводится:

– не реже одного раза в квартал;
– при внедрении новых узлов и/или технологий в ИС;
– при появлении информации о новых уязвимостях.

2.4. Анализ защищенности узлов необходимо проводить следующими механизмами:

– сканер портов;
– сканер TCP/UDP-сервисов;
– сканер уязвимостей в:
  - прикладном программном обеспечении;
  - системном программном обеспечении;
– подбор паролей.

2.5. Сканирование осуществляется изнутри локальной вычислительной сети ИС.

2.6. Сканирование ИС должно проводиться в моменты их минимальной загруженности.

2.7. По результатам каждого сканирования должен быть составлен отчет с описанием выявленных уязвимостей.

2.8. Перечень полученных уязвимостей, при наличии возможности, должен быть устранен администратором безопасности ИС в течении 1 (одного) года путем установки обновлений программного обеспечения, выпущенных производителем программного обеспечения.

2.9. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения администратор безопасности ИС должен предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

3. Регламент ввода в эксплуатацию ИС после внесения изменений

3.1. Нормативно-методической документацией определены следующие характеристики ИС, об изменениях которых требуется обязательно извещать орган по аттестации (организацию):

– состав и условия размещения технических средств и систем;

– состав (комплектность) продукции, используемой в целях защиты информации, схема ее монтажа (параметры установки и настройки), способствующие снижению уровня защищенности объекта информатизации.

3.2. Орган по аттестации (организация) принимает решение о необходимости проведения оценки соответствия ИС требованиям по защите информации после изменений вышеуказанных характеристик.

3.3. Обязательная проверка эффективности системы защиты проводится при изменении условий эксплуатации, а также технических, программных и программно-технических средств ИС, приводящих к нарушению их штатной работы, включая штатную работу системы защиты информации, или к образованию угроз безопасности информации.

3.4. Эксплуатация ИС разрешается только после проведения проверки эффективности системы защиты организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Зам. директора по БЖ А.С. Балахнин