Управление образования, молодёжной политики и спорта администрации
Амурского муниципального района Хабаровского края
Муниципальное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа пос. Известковый
Амурского муниципального района Хабаровского края
(МБОУ СОШ пос. Известковый)

ПРИНЯТО
на заседании
Педагогического совета
Протокол № 4 от 09
января 2024 г

УТВЕРЖДЕНО
приказом директора
МБОУ СОШ пос.
Известковый
№ 05-Д от 12.01.2024 г.

Положение по организации процесса управления уязвимостями в (организации)

1. Общие положения

1.1. Настоящее положение по управлению уязвимостями в (организации) (далее – Положение) разработано в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

1.2. Положение определяет состав и содержание работ по анализу и устранению уязвимостей (далее – управление уязвимостями), выявленных в программных, программно-аппаратных средствах информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, информационно-телекоммуникационных инфраструктурах центров обработки данных, на базе которых функционируют эти системы и сети (далее – информационные системы).

1.3. Настоящее Положение подлежит применению организациями при принятии ими мер по устранению уязвимостей программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, а также иными нормативными правовыми актами и методическими документами ФСТЭК России.

1.4. Цель Положения является устранение уязвимостей.

1.5. Управление уязвимостями сертифицированных программных, программно-аппаратных средств защиты информации обеспечивается с учетом эксплуатационной документации на них, а также рекомендаций разработчиков.

2. Нормативные ссылки

2.1. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»,

2.2. ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»,

2.3. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»,

2.4. ГОСТ Р 59547-2021 «Мониторинг информационной безопасности»

2.5. ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения»

иными национальными стандартами в области защиты информации и обеспечения информационной безопасности.

2.6. Методика тестирования обновлений безопасности программных, программно-аппаратных средств (утвержден ФСТЭК России 28 октября 2022 г.);

2.7 Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств (утвержден ФСТЭК России 28 октября 2022 г.);

2.8. Руководство по организации процесса управления уязвимостями в органе (организации) (утвержден ФСТЭК России 17 мая 2023 г.).

3. Процесс управления уязвимостями

3.1. Процесс управления уязвимостями включает пять основных этапов.

Этапы работ по управлению уязвимостями:

1. Мониторинг уязвимостей и оценка их применимости

На этапе мониторинга уязвимостей и оценки их применимости осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников, и принятие решений по их последующей обработке.

2. Оценка уязвимостей

На этапе оценки уязвимостей определяется уровень критичности уязвимостей применительно к информационным системам органа (организации).

3.Определение методов и приоритетов устранения уязвимостей

На этапе определения методов и приоритетов устранения уязвимостей определяется приоритетность устранения уязвимостей и выбираются методы их устранения: обновление программного обеспечения и (или) применение компенсирующих мер защиты информации.

4. Устранение уязвимостей

На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

5. Контроль устранения уязвимостей

На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о процессе управления уязвимостями и его результатах, а также принятие решений по улучшению данного процесса.

3.2. Процесс управления уязвимостями организуется для всех информационных систем (организации) и предусматривает постоянную и непрерывную актуализацию сведений об уязвимостях и объектах информационной системы.

4. Участниками процесса управления уязвимостями являются:

- руководитель;
- специалист, ответственный за проведение оценки угроз безопасности информации (далее – аналитик угроз);
- специалист, ответственный за проведение оценки защищенности;
- специалист, ответственный за внедрение мер защиты информации; (системный администратор учреждения).

По решению руководителя (организации) в процессе управления уязвимостями могут быть задействованы другие подразделения и специалисты, в частности, подразделение, ответственное за организацию закупок программных и программно-аппаратных средств, подразделение, ответственное за эксплуатацию инженерных систем. Распределение операций, реализуемых в рамках процесса управления уязвимостями, по ролям работников подразделений ИТ и подразделения по защите (организации).

5. Устранение уязвимостей

Процесс устранения уязвимостей осуществляется в соответствии с методическими документами, разработанными Управлением ФСТЭК России для обеспечения адаптации организационно-распорядительных документов, регламентирующих процессы выявления, анализа и устранения уязвимостей.

6. Порядок пересмотра Положения

6.1 При возникновении необходимости в Положение вносятся изменения.

6.2 Инициатором внесения изменений в Положение может быть управление образования, молодежной политики и спорта администрации Амурского муниципального района, путем направления информационного письма на имя Директора по эксплуатации систем информационной безопасности с обоснованием необходимости пересмотра Положения.

7. Контроль

7.1 Контроль за соблюдением пунктов Положения осуществляется специалистом по информационной безопасности (системным администратором учреждения).

7.2 В рамках проведения процедур идентификации и анализа уязвимостей информационной безопасности (специалист по информационной безопасности (системный администратор учреждения). имеет право применять все необходимые программные и технические средства включая те, на которые установлен запрет иными локальными нормативными актами учреждения.

7.3 С целью контроля за эффективностью процесса управления уязвимостями информационной безопасности не реже 1 раза в год должен проводится независимый тест на проникновение.

7.4 Специалист по информационной безопасности (системный администратор учреждения) в случае обнаружения фактов нарушения пунктов

Положения, возникших в связи с недобросовестным исполнением Участниками Процесса своих обязанностей в рамках Положения или возникших в результате нарушения нормативных документов учреждения в области информационной безопасности, сообщает о данных фактах вышестоящему руководителю сотрудника, нарушившего пункты Положения.

8. Ответственность

8.1 Участники процесса управления уязвимостями информационной безопасности учреждения несут персональную ответственность за соблюдение пунктов Положения.

8.2 К работникам, нарушившим пункты Положения могут применяться дисциплинарные взыскания в порядке, установленном законодательством Российской Федерации.

8.3 Ответственность третьих лиц, включая сотрудников подрядных организаций, должны учитываться в договорах (соглашениях), заключенных с ними. Ответственность за включение положений настоящего Положения лежит на руководителе учреждения.

Управляющим советом
(протокол от 14.09.2023 № 3)