**Об утверждении Регламента д****еятельности по выявлению, анализу   
и устранению критичных уязвимостей в информационных системах, эксплуатируемых в ФГБУ «Заповедное Подлеморье»**

В целях повышения эффективности обеспечения информационной безопасности в ФГБУ «Заповедное Подлеморье», во исполнение пункта 2 приказа Минприроды России от 31.08.2023 № 566 «Об утверждении Регламента деятельности по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в ФГБУ «Заповедное Подлеморье» приказываю:

1. Утвердить прилагаемый Регламент деятельности по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в ФГБУ «Заповедное Подлеморье».

2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор

ФГБУ «Заповедное Подлеморье» М.Е.Овдин

|  |  |
| --- | --- |
|  | Утвержден приказом  ФГБУ «Заповедное Подлеморье»  от \_\_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_ |

**РЕГЛАМЕНТ ДЕЯТЕЛЬНОСТИ ПО ВЫЯВЛЕНИЮ, АНАЛИЗУ  
И УСТРАНЕНИЮ КРИТИЧНЫХ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ, ЭКСПЛУАТИРУЕМЫХ В ФГБУ «ЗАПОВЕДНОЕ ПОДЛЕМОРЬЕ»**

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
   1. Настоящий регламент разработан на основе Руководства по организации процесса управления уязвимостями в органе (организации), утвержденного ФСТЭК России от 17 мая 2023 г и определяет состав и содержание работ по анализу и устранению уязвимостей, выявленных в информационных системах ФГБУ «Заповедное Подлеморье».
   2. Целью данного регламента является обеспечение безопасности и защиты информации, хранимой и обрабатываемой в информационных системах .
   3. Настоящий регламент подлежит применению ФГБУ «Заповедное Подлеморье». при принятии мер по устранению уязвимостей программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, а также иными нормативными правовыми актами и методическими документами ФСТЭК России.

1.4. Процесс анализа и устранения уязвимостей включает пять основных этапов: мониторинг уязвимостей и оценки их применимости, оценка уязвимостей, определение методов и приоритетов устранения уязвимостей, устранение уязвимостей и контроль устранения уязвимостей.

1. **ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ**

2.1. Выявление уязвимостей осуществляется на этапе мониторинга уязвимостей и оценки их применимости на основании данных из следующих источников:

а) внутренние источники:

системы управления информационной инфраструктурой (далее – ИТ-инфраструктура);

базы данных управления конфигурациями;

документация на информационные системы;

б) база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации (далее – БДУ) ФСТЭК России;

в) внешние источники:

базы данных, содержащие сведения об известных уязвимостях;

официальные информационные ресурсы разработчиков программных и программно-аппаратных средств и исследователей в области информационной безопасности.

2.2. На этапе мониторинга уязвимостей и оценки их применимости выполняются операции, приведенные в таблице 1.

Таблица 1

|  |  |  |
| --- | --- | --- |
| №  п/п | Наименование  операции | Описание операции |
|  | Анализ  информации об  уязвимости | Анализ информации из различных источников c целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к информационным системам ФГБУ «Заповедное Подлеморье». Агрегирование и корреляция собираемых данных об уязвимостях |
|  | Оценка применимости  уязвимости | На основе информации об объектах информационных систем и их состоянии определяется применимость уязвимости к информационным системам ФГБУ «Заповедное Подлеморье» с целью определения уязвимостей, не требующих дальнейшей обработки (не релевантных уязвимостей). Оценка применимости уязвимостей производится:  на основе анализа данных об ИТ-инфраструктуре;  на основе анализа данных о возможных объектах воздействия. |

1. **АНАЛИЗ И ОЦЕНКА УЯЗВИМОСТЕЙ**

3.1. С целью определения уровня критичности уязвимостей применительно к информационным системам ФГБУ «Заповедное Подлеморье» производится анализ и оценка уязвимостей.

3.2. Оценка уровня критичности уязвимостей в информационных системах ФГБУ «Заповедное Подлеморье» проводится в соответствии с Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28.10.2022.

3.3. На этапе оценки уязвимостей выполняются операции, приведенные в таблице 2

Таблица 2

|  |  |  |
| --- | --- | --- |
| №  п/п | Наименование  операции | Описание операции |
|  | Получение информации об объектах, подверженных  уязвимости | Получение выборки объектов информационных систем, подверженных уязвимости |
|  | Определение уровня опасности уязвимости | Расчет базовой, контекстной и временной метрик по методике CVSS с использованием калькулятора CVSS V3 или V3.1, размещенного в БДУ ФСТЭК России |
|  | Определение влияния на информационные системы | Определение влияния уязвимого компонента на защищенность информационных систем |
|  | Расчет критичности уязвимости | Получение значений уровней критичности обнаруженных уязвимостей |

1. **УСТРАНЕНИЕ УЯЗВИМОСТЕЙ**
   1. Приоритетность устранения уязвимостей и выбор методов их устранения (обновление программного обеспечения и (или) применение компенсирующих мер защиты информации) осуществляются на этапе определения методов и приоритетов устранения уязвимостей.
   2. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) уязвимостей, выявленные на этапе мониторинга. При этом выполняются операции, представленные в таблице 3.

Таблица 3.

|  |  |  |
| --- | --- | --- |
| №  п/п | Наименование  операции | Описание операции |
|  | Тестирование обновления | Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации (далее – недекларированные возможности) |
|  | Установка обновления в тестовом сегменте | Установка обновлений на выбранном тестовом сегменте информационной системы в целях определения влияния их установки на ее функционирование |
|  | Принятие решения об установке обновления | В случае, если негативного влияния от установки обновления на выбранном сегменте системы не выявлено, принимается решение о его распространении в системе. В случае обнаружения негативного влияния от установки обновления на выбранном сегменте системы дальнейшее распространение обновления не осуществляется, при этом для нейтрализации уязвимости применяются компенсирующие меры защиты информации |
|  | Разработка и реализация компенсирующих мер защиты информации | Разработка и применение компенсирующих мер защиты информации, которые применяются в связи с невозможностью установки обновления, обнаружением негативного влияния от установки обновления, а также в случае необходимости принятия мер до устранения уязвимости производителем.  К компенсирующим мерам защиты информации могут относиться: организационные меры защиты информации;  настройка средств защиты информации;  анализ событий безопасности;  внесение изменений в ИТ-инфраструктуру. |

* 1. Тестирование обновлений программных и программно-аппаратных средств осуществляется в соответствии с Методикой тестирования обновлений программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г., по решению ФГБУ «Заповедное Подлеморье» в случае отсутствия соответствующих результатов тестирования в БДУ ФСТЭК России.
  2. При наличии соответствующих сведений могут быть использованы компенсирующие меры защиты информации, представленные в бюллетенях безопасности разработчиков программных, программно-аппаратных средств, а также в описаниях уязвимостей, опубликованных в БДУ ФСТЭК России.
  3. Сроки устранения уязвимостей:

критический уровень опасности до 24 часов;

высокий уровень опасности – до 7 дней;

средний уровень опасности – до 4 недель;

низкий уровень опасности – до 4 месяцев.