ПЛАНИРОВАНИЕ ПРОЦЕССА УСТРАНЕНИЯ УЯЗВИМОСТЕЙ. ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Ведущий специалист по защите информации
Мезинова Наталья Алексеевна

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

НОРМАТИВНО-МЕТОДИЧЕСКИЕ ТРЕБОВАНИЯ ПРИ ПЛАНИРОВАНИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

ДИТ

Методический документ

«Руководство по организации процесса управления уязвимостями в органе (организации)»
(утв. ФСТЭК России **17.05.2023**)

Методический документ

«Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств»
(утв. ФСТЭК России **28.10.2022**)

Национальный стандарт РФ

ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей

Национальный стандарт РФ

ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем"

Справочник CVSS

Методика CVSS с использованием использованием калькулятора калькулятора CVSS V3 или V3.1, размещена в БДУ ФСТЭК России

ОЦЕНКА УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ КОМПОНЕНТА ИС

ДИТ

Определяем программные, программно-аппаратные средства подверженные уязвимостям

Определяем место размещения компонентов в ИС

Определяем уровень опасности уязвимости по методике **CVSS 3.0** или **3.1**

Определяем влияние уязвимости программных, программно-аппаратных средств на функционирование ИС

Рассчитываем уровень критичности уязвимости программных, программно-аппаратных средств в ИС

По результатам расчета мы получаем уровень критичности уязвимости компонента применительно к конкретной ИС

ПРОБЛЕМЫ ПРИ ПЛАНИРОВАНИИ ПРИОРИТЕТА УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

ДИТ

$V_{уз1} = V_{узn} = 10$	Одномоментное устранение нескольких уязвимостей одинакового уровня критичности в ИС
$V_{уз} = 10 \rightarrow C_{г1}, C_{г2}, C_{гn}$	Сегментация ИС
$T_о < T_у$	Ограниченная длительность «технологических окон»

ПУТИ РЕШЕНИЯ

ДИТ

При определении приоритета устранения уязвимостями в ИС учитывать дополнительные параметры:

Статические показатели
для конкретной ИС или ее сегментов (важность сегментов)

Динамические показатели (ресурсы, внешние ограничения, транспортная доступность и т.д.)

Приоритезация позволит обоснованно принимать оптимальные решения руководителям подразделений безопасности на этапе планирования процесса устранения уязвимостей в ИС

ВСЕГДА НА СВЯЗИ!

ДЕПАРТАМЕНТ
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ

@DIT_MOSCOW