ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

СИТУАЦИОННЫЙ ПОДХОД К ПОСТРОЕНИЮ МОДЕЛИ ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

- МАМУТА В.В. СОЛОВЬЕВ С.В.

Докладчик:

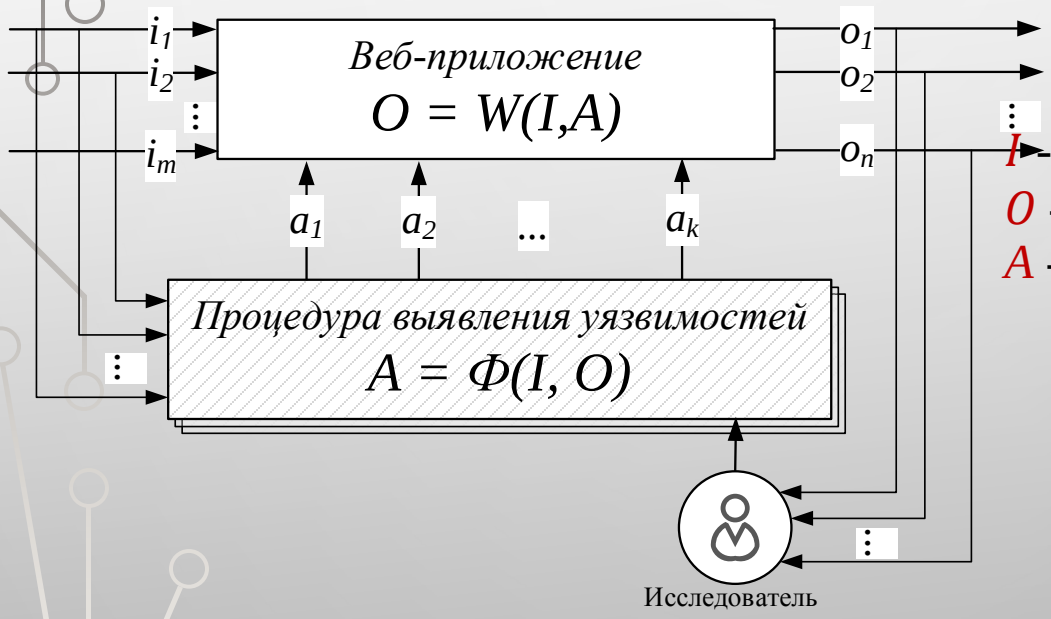
доктор техн. наук, проф. Язов Юрий Константинович

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

ОБЩАЯ СХЕМА ИССЛЕДОВАНИЙ

ЭТАП 1 Подготовка к проведению исследований

ЭТАП 2 Проведение исследований



I - множество входных данных

O - множество выходных данных

A - множество воздействий

Критерий проведения исследований (Φ) – *максимизация проверенных параметров* за время проведения исследований

ЭТАП 3 Оформление результатов исследований

ЛОГИКО-ЛИНГВИСТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ

Фаза 1. *Определение входных точек веб-приложения.*

Ситуации $\dot{Q}_1 - \dot{Q}_{10}$. Пример:

$$\dot{Q}_1 = ((m_9 x_{25}) r_{77} x_{24})$$

x_{25} – понятие «HTTP-метод», m_9 – модификатор «метод GET», r_{77} – отношение «быть способом передачи данных», x_{24} – понятие «входная точка»

Фаза 2. *Анализ использования передаваемых параметров.*

Ситуации $\ddot{Q}_1 - \ddot{Q}_{39}$, $\ddot{Q}_1^1 - \ddot{Q}_6^1$ и $\ddot{Q}_1^2$. Пример:

$$\ddot{Q}_7 = ((v r_{38} x_7)((x_6 r_9 x_7)(x_6 r_2 x_8)))$$

v – понятие «пользовательский ввод», x_6 – атрибут тега, x_7 – понятие «значение атрибута тега», x_8 – понятие «атрибут-событие», r_2 – отношение «быть элементом класса», r_9 – отношение «признак-значение», r_{38} – отношение «быть внутри (в пространстве)»

Фаза 3. *Подтверждение потенциальных уязвимостей.*

Ситуации $\dddot{Q}_1 - \dddot{Q}_6$. Пример:

$$\dddot{Q}_1 = ((m_3 x_{18}) r_{71} d_3)$$

x_{18} – понятие «конструкция для исполнения кода», m_3 – модификатор «конструкция в виде HTML-тега», r_{71} – отношение «иметь объектом действия», d_3 – действие «выполнение сценария в браузере»

ОБОБЩЕНИЕ СИТУАЦИЙ. УНИВЕРСАЛЬНЫЕ ИНТЕРПРЕТИРУЕМЫЕ КОНСТРУКЦИИ (УИК)

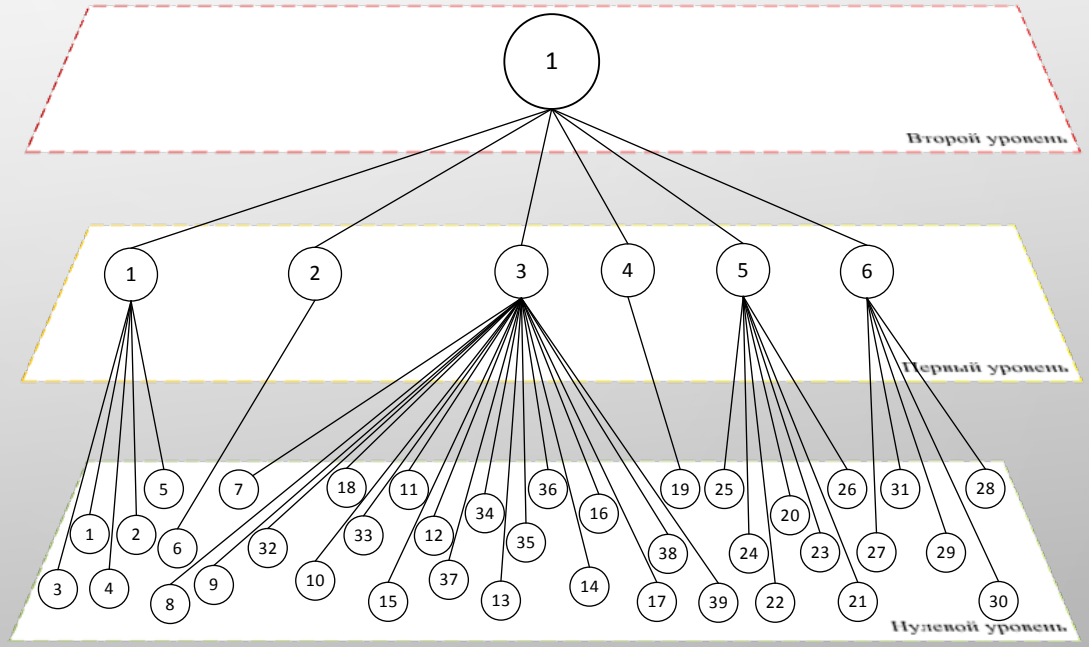
Фаза 2. *Три уровня обобщения ситуаций.*

Обобщенное описание второго уровня:

$$\ddot{Q}_1^2 = (vr_{42}\xi_5)$$

Обобщенные описания первого уровня $\ddot{Q}_1^1 - \ddot{Q}_6^1$

Исходные описания ситуаций $\ddot{Q}_1, \ldots, \ddot{Q}_{39}$



Пример УИК:

Контекст URI | Контекст атрибутов | Контекст комментариев HTML | Внедряемый код

javascript:(onclick=prompt(1))'"></textarea/</title/</style/</script/-->\x3csvg<svg/onload=prompt(2)>\x3e

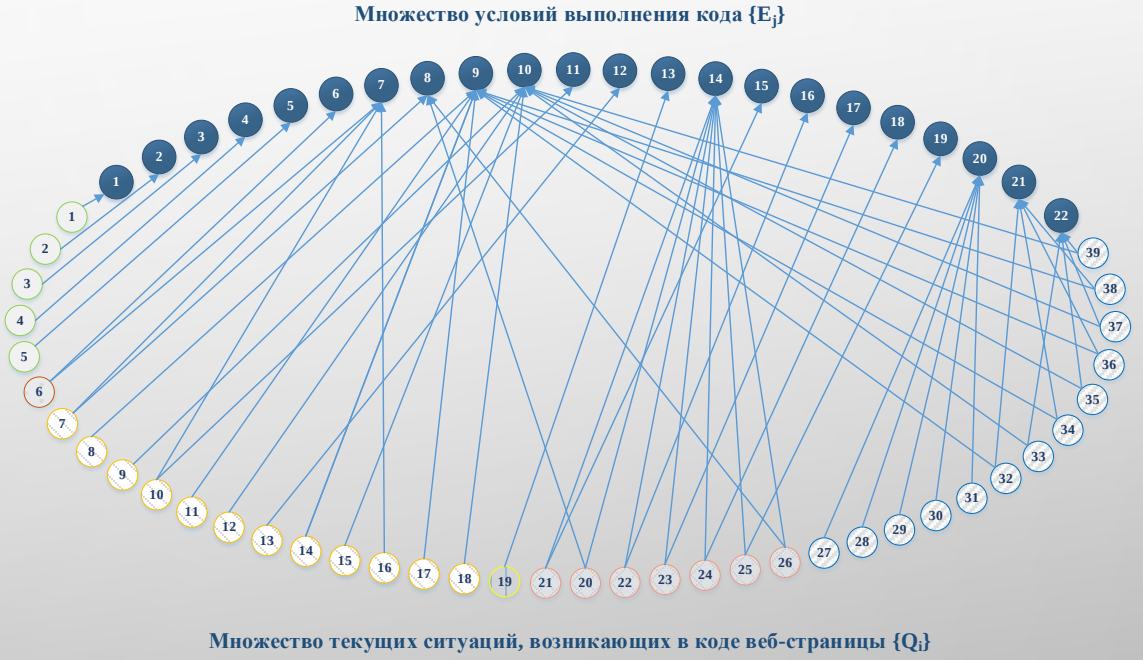
Псевдо-протокол | Контекст имени атрибута | Контекст HTML-тегов | «<» | Исполняемый код | «>»

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

ПОПОЛНЕНИЕ ОПИСАНИЙ СИТУАЦИЙ

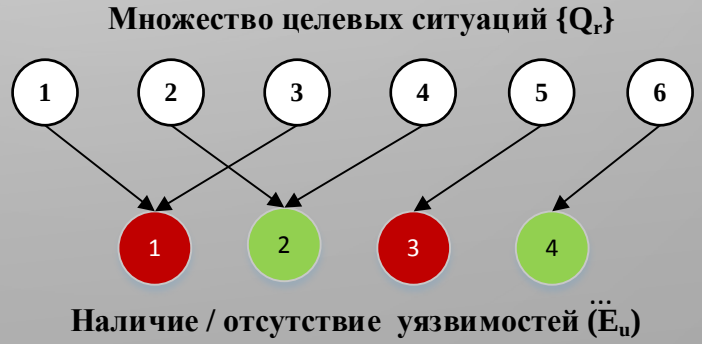
Фаза 2. *Сценарий пополнения описаний ситуаций*:

Образование полных ситуаций, которым соответствуют определенные действия исследователя



Фаза 3. *Сценарий пополнения описаний ситуаций*:

Получаемые продукции опеделяют наличие или отсутствие уязвимостей



СПАСИБО ЗА ВНИМАНИЕ!

zolton007@mail.ru

Язов Юрий Константинович