О МЕТОДИКЕ ИДЕНТИФИКАЦИИ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ УЯЗВИМОСТЕЙ

И.Ю. Богомазова (ст. гр. КЗИ-108)[1]
Научный руководитель: *Д.В. Мишин* (ст. преп. каф. ИЗИ)[2]
[1] *Факультет информационных технологий, кафедра ИЗИ, специальность 090104, e-mail: xoofari@yandex.ru*
[2] *Факультет информационных технологий, кафедра ИЗИ, старший преподаватель, e-mail: mishin.izi@gmail.com*

Аннотация – В работе предлагается методика идентификации уязвимостей на основе значения уязвимостей. Представлены формулы для расчета значения уязвимости. Описана возможность применения данной методики в аудите информационной безопасности. Дано упрощенное представление модели в виде дерева.

Ключевые слова – информационная безопасность, уязвимость, идентификация, методика, значение, дерево.

Abstracts – This paper proposes the method of identification of vulnerabilities based on the vulnerabilities importance. There are the formulas for calculating the vulnerabilities importance in it. Also it describes the possibility of using this method in the information security audit. We presented the simplified representation of a model as a graph.

Keywords – information security, vulnerability, identification, method, importance, graph.

Защищенность объекта информатизации напрямую зависит от наличия различного рода уязвимостей его активов. Поэтому одним из важнейших этапов аудита информационной безопасности предприятия является нахождение уязвимостей, присущих данной системе и ее составляющим [1]. Для решения данной задачи широко применяется метод опроса сотрудников и аудиторов [2]. Но нет общей универсальной концепции идентификации уязвимостей, что связано с недостаточным развитием научной базы в области информационной безопасности.

Авторами предлагается методика идентификации уязвимостей на основе расчета их значения.

Представим всю совокупность уязвимостей в виде множества (1)

$$V = \{v_1, v_2, ..., v_n\}, \quad (1)$$

где $n \in N$ – мощность множества V.

Введем понятие значение (вес) уязвимости. Предполагаем, что одна и та же уязвимость, находящаяся в разных контекстах, может проявляться более или менее. Такой качественной оценке сопоставим количественный эквивалент (2)

$$g_{v_i} \in [0;1]. \quad (2)$$

По этому значению предполагается судить о степени присутствия той или иной уязвимости.

Определим следующие правила:

Правило 1: Пусть данная уязвимость отсутствует для определенного элемента информационной системы (ИС), тогда значение этой уязвимости для этого элемента равно 0. Правило имеет и обратный характер.

Правило 2: Если уязвимость полностью проявляется, тогда ее значение $g_{v_i} = 1$. Правило также имеет обратный характер.

Считаем, что каждая i-я уязвимость ($i=\overline{1,n}$) может быть однозначно идентифицирована по $k_i \in N$ признакам. Множество возможных идентификационных признаков уязвимостей обозначим (3)

$$F = \{f_1, f_2, ..., f_p\}. \quad (3)$$

Таким образом, каждому элементу $v_i \in V$ ставится в соответствие определенное подмножество $A_i \in F$, $|A_i| = k_i$ множества F.

$$l_V : V \to 2^F. \quad (4)$$

Формула (4) описывает многозначное отображение, отражающее выбор критериев для определения уязвимости, где

2^F — совокупность всех подмножеств множества F.

Введем дополнительные категории:

- элемент признака (критерия),
- значение элемента признака (5)

$$g_{e_q} \in \{0, g_{e_q}^{max}\}, \quad (5)$$

- значение признака (6)

$$g_{f_j} \in [0; g_{f_j}^{max}]. \quad (6)$$

Элемент признака уточняет данный признак.

$$E = \{e_1, e_2, ..., e_z\}. \quad (7)$$

Обозначим (7) – множество элементов признаков. Для каждого признака определено свое подмножество элементов $B_j \subset E$, $|B_j| = s_j$.

$$l_F : F \to 2^E. \quad (8)$$

(8) - многозначное отображение, описывающее выбор элементов признаков, где

2^E — совокупность всех подмножеств множества E.

Каждый признак обладает определенным максимальным значением $g_{f_j}^{max}$ таким, что сумма максимальных значений всех признаков данной уязвимости (i-ой) равна 1 (9):

$$\sum_{j=1}^{k_i} g_{f_j}^{max} = 1. \quad (9)$$

Максимальный вес признака определяется экспертами на основе влияния данного признака (при его полном присутствии) на значение уязвимости.

В свою очередь каждый элемент признака также обладает максимальным значением $g_{e_q}^{max}$, которое определяется экспертами по вкладу элемента в значимость признака. Сумма значений всех элементов признака должна быть равна максимальному значению этого признака (10):

$$\sum_{q=1}^{s_j} g_{e_q}^{max} = g_{f_j}^{max}. \quad (10)$$

Значение признака в таком случае (11):

$$g_{f_j} = \sum_{q=1}^{s_j} g_{e_q}. \quad (11)$$

Если некоторый элемент признака при анализе не обнаружен, то его значение (12) должно быть приравнено к 0:

$$g_{e_q} = 0. \quad (12)$$

Значение i-ой уязвимости в текущем контексте определяется по формуле (13):

$$g_{v_i} = \sum_{j=1}^{k_i} g_{f_j} = \sum_{j=1}^{k_i} \sum_{q=1}^{s_j} g_{e_q}. \quad (13)$$

Наличие правил позволяет применять разработанную модель для идентификации уязвимостей элементов ИС.

Основываясь на предложенной модели, можно составить анкету для опроса сотрудников организации или аудиторов с целью определить существующие на предприятии уязвимости. В качестве вопросов могут выступать признаки уязвимости, вариантами ответа в таком случае должны быть элементы данного признака. Рассчитав значение уязвимости g_{v_i} по формуле (13), получим степень присутствия данной уязвимости в элементе системы. Если g_{v_i} приближается к 0, то можно считать, что данная уязвимость для определенного элемента системы отсутствует.

Для наглядности представим описанную выше модель для одной составляющей ИС и одной ее уязвимости в виде дерева. Вершины дерева: уязвимость, признаки и элементы признаков. Корень дерева – составляющая ИС (например, техническое средство и т.п., обозначена o_1). Отношения между сущностями представляются ребрами, соединяющими соответствующие вершины.

Ребра снабжены весами:

- Ребра между составляющей ИС и уязвимостью имеют вес g_{v_i}.
- Ребра между уязвимостью и признаками имеют вес g_{f_j}.
- Ребра между признаками и элементами признаков имеют вес g_{e_q}.

Дерево представлено на рисунке 1.

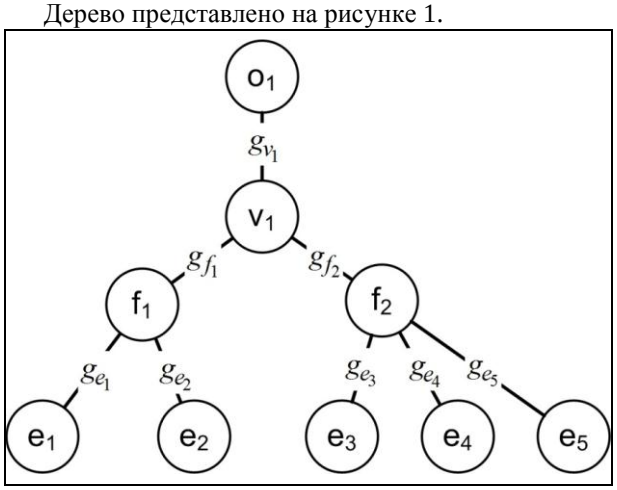

Рисунок 1 – Представление разработанной модели в виде дерева

Таким образом, в работе представлена методика идентификации уязвимостей, основанная на расчете значения уязвимости. Описан порядок применения данной методики для составления анкет для опроса сотрудников и аудиторов. Значения уязвимостей, поученные после анализа опросных листов, могут быть учтены при расчете защищенности информационных ресурсов на данном предприятии. Разработанная методика может найти применение в автоматизированной системе анализа защищенности объекта информатизации.

Список использованных источников

[1] Курило А.П. Аудит информационной безопасности / А. П. Курило, С. Л. Зефиров, В. Б. Голованов. – М.: БДЦ-Пресс, 2006. – 304 с.

[2] Астахов А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.