УДК 681.3.06

О.Е. Мазулевский

Полтавский военный институт связи

МЕТОДИКА ФОРМИРОВАНИЯ ПЛАНА ДЕЙСТВИЙ АДМИНИСТРАТОРА ПО РЕЗУЛЬТАТАМ КОНТРОЛЯ ЗАЩИЩЕННОСТИ

В статье рассмотрен подход к решению задачи формирования плана действий администратора для устранения уязвимостей защиты компьютерной сети, обнаруженных в результате контроля. Приведенная методика позволяет в режиме реального времени проводить формирование последовательности действий администратора для устранения обнаруженных уязвимостей.

план действия, администратор, результаты контроля, защищенность

Введение

Одним из этапов деятельности администратора безопасности при проведении контроля защищенности компьютерной сети является этап информационной подготовки принятия решения по устранению обнаруженных уязвимостей [1]. Сущность данного этапа заключается в изучении, анализе и обобщении администратором отчетной информации, сформированной по результатам контроля с целью разработки плана действий по устранению найденных уязвимостей. При этом администратор вынужден выполнять рутинные ручные операции по корректировке отображаемой информации, а именно: изменению формы её представления и содержания, что приводит к нерациональному использованию его интеллектуальных возможностей и снижению творческого потенциала. Кроме того, задача составления плана действий усложняется необходимостью отслеживания версий установленных программных продуктов и необходимостью соблюдения очередности установки обновлений.

Задача формирования плана действий заключается в определении порядка действий администратора и относится к классу задач составления расписания. Такие задачи не поддаются решению аналитическими методами, считаются традиционно трудноразрешимыми и являются NP-полными [2, 3]. Для их решения существуют точные и приближенные методы, например, логического программирования в ограничениях, метод отжига, алгоритмы раскраски графов, генетические алгоритмы и методы имитационного моделирования [2 – 6]. Использование точных методов в данном случае неприемлемо, так как они не предназначены для реализации в реальном времени вследствие их сложности и большого времени решения задачи. В работах [2, 6] рассмотрен вариант решения, основанный на методах приближенного динамического программирования, что обуславливает возможность их применение в системах реального времени. Однако, в данном случае, требуется задание значения директивного времени выполнения действий и не учитываются ограничения на последовательность их выполнения.

В основу предлагаемой методики формирования плана действий администратора, положен один из методов решения оптимизационных задач базирующийся на «жадном» алгоритме [7, 8]. Такой алгоритм делает на каждом шаге локально оптимальный выбор, допуская, что итоговое решение также окажется оптимальным. Решение, принимаемое на каждом шаге должно быть оптимальным только на текущем шаге и должно приниматься без учета предыдущих или последующих решений.

В нашем случае предполагается применить жадный алгоритм на последнем этапе формирования плана действий администратора безопасности по результатам контроля.

Описание методики

Исходные данные и постановка задачи. Пусть дано множество $S = \{s_i\}$ узлов компьютерной сети, $i = \overline{1, I}$; множество $P = \{p_j\}$ проверок предназначенных для проведения контроля защищенности узлов компьютерной сети, $j = \overline{1, J}$; матрица $O \equiv \{o_{ij}\}$ результатов контроля защищенности компьютерной сети. Каждый элемент матрицы принимает следующие значения

$$o_{ij} = \begin{cases} 1, \text{если } j\text{-я уязвимость найдена на } i\text{-м узле}, \\ 0 \text{ в противном случае}; \end{cases}$$

φ_m – действия администратора безопасности по устранению обнаруженных уязвимостей; $\Lambda = \{\lambda_j\}$ – система множеств, элементы которых определяют ограничения на очередность выполнения отдельных действий φ_m.

Необходимо сформировать план Φ действий φ_m администратора безопасности по устранению обнаруженных уязвимостей, т.е. $\Phi = \{\varphi_1, \ldots, \varphi_m, \ldots, \varphi_M\}$, $m = \overline{1, M}$, при условии устранения в первую очередь важных уязвимостей и выполнении ограничений на очередность их устранения. Методика включает следующие этапы.

Этап формирования групп действий. Группа b_{ik} образуется при применении к действиям φ_m, которые необходимо выполнить на s_i узле сети, огра-

ничения λ_j, задающего жесткий порядок выполнения действий в группе

$$b_{ik} := b_{ik} \cup \varphi_m \left| \begin{array}{l} \varphi_m \subseteq \lambda_j; \\ j = m. \end{array} \right.$$

Под ограничениями λ_j понимается множество, включающее номера действий которые необходимо выполнить перед выполнением действия с порядковым номером j. Например, если $\lambda_5 = \{1, 2, 6\}$, то это значит, что перед выполнением действия предназначенного для устранения уязвимости с номером 5 необходимо выполнить действия по устранению уязвимостей с номерами 1, 2 и 6. Между группами ограничения на порядок выполнения действий отсутствуют, поэтому каждая группа может выполняться независимо.

При устранении j-й уязвимости может возникнуть необходимость выполнить дополнительные, вспомогательные действия, связанные с установкой необходимых обновлений для используемого на s_i узле сети программного обеспечения. Решить данную задачу можно на основе сведений, хранящихся в электронном паспорте узла. Такими сведениями, например, могут быть дата установки, тип и версия установленного программного обеспечения, а также сведения об особенностях аппаратных компонентах узла.

Этап формирования подпрограмм действий. Под подпрограммой действий будем понимать совокупность групп действий отобранных по максимальному значению некоторого показателя. В качестве такого показателя для j-го действия будем использовать значение обобщенного показателя c_j влияния j-й уязвимости на защищенность компьютерной сети. Введем три уровня для оценки значения показателя c_j: низкий, средний и высокий. Тогда можно сформировать три подпрограммы действий, соответствующих данных уровням – Ξ^B, Ξ^C, Ξ^H. Подпрограмма действий Ξ^B будет включать группы, у которых максимальная оценка обобщенного показателя имеет высокий уровень. Подпрограмма действий Ξ^C будет включать группы, у которых максимальная оценка обобщенного показателя имеет средний уровень. Подпрограмма действий Ξ^H будет включать группы, у которых максимальная оценка обобщенного показателя имеет низкий уровень.

Таким образом, первым шагом для формирования подпрограмм действий является определение c_j – обобщенного показателя влияния уязвимости на защищенность компьютерной сети.

Для определения c_j введем вектор параметров $G^0 \equiv \{g_1^0, g_2^0, g_3^0\}$, характеризующих уязвимость, представленный лингвистическими переменными: g_1^0 – «степень опасности уязвимости», g_2^0 – «простота реализации атаки с использованием уязвимости», g_3^0 – «популярность (частота) использования уязвимости». Значения функций принадлежности лингвистических переменных содержаться для каждой проверки в векторе $G^j \equiv \{g_1^j, g_2^j, g_3^j\}$.

Обозначим через вектор $C \equiv \{c_j\}$ обобщенных показателей влияния уязвимостей обнаруженных в результате контроля на защищенность компьютерной сети. Количественные значения частных показателей задаются по результатам проведения экспертного опроса, путем преобразования нечетких высказываний экспертов в определенные значения и оцениваются числами, лежащими на интервале [0, 1]. Тогда, обобщенный показатель влияния уязвимости, обнаруживаемой j-й проверкой на защищенность компьютерной сети, будет определяться с помощью аддитивного показателя

$$c_j = \sum_{n=1}^{N} g_n^j \varepsilon_n ,$$

где c_j – значения обобщенного показателя для j-й уязвимости, g_n^j – значения n-х частных показателей для j-ой уязвимости, ε_n – весовые коэффициенты n-х частных показателей. Весовой коэффициент имеет тем большую величину, чем большее влияние он оказывает на важность показателя, при этом:

$$\sum_{n=1}^{N} \varepsilon_n = 1 ; \ \varepsilon_n > 0 ; \ N = 3; \ n = 1, 2, 3.$$

Определение весовых коэффициентов для частных показателей может производиться различными методами, например, методом парных сравнений (метод Саати) [2, 6] либо методами, представленными в [10].

Для оценки групп действий по степени важности обобщенного показателя влияния уязвимости на защищенность компьютерной сети введем следующую шкалу (рис. 1).

Для соблюдения требования необходимости устранения в первую очередь важных уязвимостей выполним анализ каждой группы на наличие действия, степень важности обобщенного показателя у которого выше, чем у действий, следующих за ним.

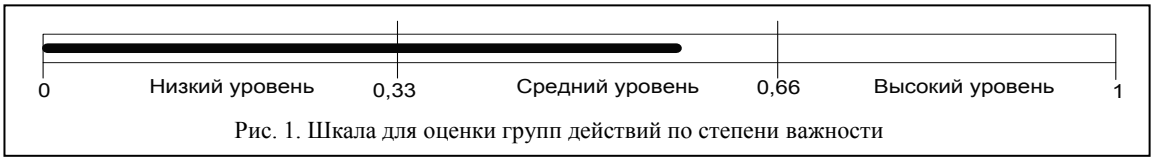

Рис. 1. Шкала для оценки групп действий по степени важности

В случае нахождения такой группы создаём новую группу. В эту группу переносим действия, стоящие после действия с максимальным значением обобщенного показателя. Таким образом, в первую очередь при формировании плана будут учтены действия, имеющие более высокий уровень обоб-

щенного показателя.

Сформируем подпрограммы действий Ξ^B, Ξ^C, Ξ^H. Правила формирования подпрограмм в формальной записи имеют такой вид:

$$\begin{aligned}\Xi^B &:= \Xi^B \cup b_{ik} \left| \max\{c_j \in b_{ik}\} \Leftrightarrow \text{"высокая"}; \right. \\ \Xi^C &:= \Xi^C \cup b_{ik} \left| \max\{c_j \in b_{ik}\} \Leftrightarrow \text{"средняя"}; \right. \\ \Xi^H &:= \Xi^H \cup b_{ik} \left| \max\{c_j \in b_{ik}\} \Leftrightarrow \text{"низкая"}. \right.\end{aligned} \quad (1)$$

Этап формирования плана действий администратора. Следующим шагом является определение критерия для работы жадного алгоритма. Данный критерий должен учитывать критичность уязвимостей устраняемых с помощью действий в группах, так же он должен учитывать незащищенность узлов, на которых будут выполняться действия, так как в большинстве случаев злоумышленники пытаются проникнуть на узлы с большим числом уязвимостей.

В качестве такого критерия будем использовать значение следующего мультипликативного показателя

$$u_{ik} = v_{ik} \times s_i^{\text{нз}},$$

где v_{ik} – усредненный обобщенный показатель группы, $s_i^{\text{нз}}$ – коэффициент незащищенности узла, значение которого позволяет получить представление об общем весе обнаруженных уязвимостей на данном узле. Выражение для расчета среднего обобщенного показателя группы v_{ik} имеет следующий вид

$$v_{ik} = \frac{\sum_{j=1}^{|b_{ik}|} c_j}{|b_{ik}|},$$

где обобщенный показатель c_j относится к действию $\varphi_m \in b_{ik}$.

Коэффициент незащищенности узла определяется по формуле

$$s_i^{\text{нз}} = \sum_{j=1}^{J} o_{ij} c_j .$$

Зная состав групп в каждой подпрограмме Ξ^B, Ξ^C, Ξ^H, на основании мультипликативного показателя u_{ik}, по жадному алгоритму, предусматривающему на каждом шаге выбор наилучшего варианта, формируется план действий администратора $\Phi = \{\varphi_1, \ldots, \varphi_m, \ldots, \varphi_M\}$, $m = \overline{1, M}$. В первую очередь в план включаются действия входящие в состав групп, в порядке их ранжирования, из состава подпрограммы Ξ^B, далее действия из групп подпрограмм Ξ^C и Ξ^H.

Таким образом, формирование плана действий администратором безопасности по результатам проведенного контроля будет проводиться в следующем порядке:

1. Фиксируются уязвимости обнаруженные на этапе проведения контроля защищенности и сопоставляются необходимые действия для их устранения.

2. На основании ограничений на порядок устранения уязвимостей формируются группы действий, с таким учетом, что каждая группа может выполняться независимо друг от друга.

3. Для каждой уязвимости и каждого соответствующего действия рассчитывается значение обобщенного показателя и проводится лингвистическая оценка.

4. На основании лингвистической оценки проводится уточнение количества групп, с целью ускорить в дальнейшем устранение критических уязвимостей.

5. На основании лингвистической оценки проводится формирование подпрограмм действий по максимальному значению обобщенного показателя в группе.

6. Определение коэффициентов незащищенности узлов сети, усредненных показателей групп действий и на их основе определение мультипликативного показателя групп действий.

7. Нахождение группы с максимальным значением мультипликативного показателя в подпрограмме с группами, содержащими действия, устраняющие уязвимости с ВЫСОКОЙ степенью критичности.

8. Включение действий найденной группы в программу действий по ограничению на порядок следования. Если группы в подпрограмме есть – переходим к предыдущему шагу, иначе следуем дальше.

9. Нахождение группы с максимальным значением мультипликативного показателя в подпрограмме с группами содержащими действия устраняющее уязвимости со СРЕДНЕЙ степенью критичности.

10. Включение действий найденной группы в программу действий по ограничению на порядок следования. Если группы в подпрограмме есть – переходим к предыдущему шагу, иначе следуем дальше.

11. Нахождение группы с максимальным значением мультипликативного показателя в подпрограмме с группами, содержащими действия устраняющие уязвимости с НИЗКОЙ степенью критичности.

12. Включение действий найденной группы в программу действий по ограничению на порядок следования. Если группы в подпрограмме есть – переходим к предыдущему шагу, иначе останов.

Рассмотрим **пример составления плана действий администратора** безопасности при устранении обнаруженных уязвимостей.

Допустим, что компьютерная сеть состоит из 6-и узлов, для контроля защищенности которых используются 7 проверок. Пусть после проведения контроля матрица результатов контроля защищенности O имеет вид:

1	0	1	0	1	0
1	0	0	0	0	1
0	1	0	1	0	1
0	0	0	1	1	0
1	0	1	0	0	1
1	0	0	0	1	0

1	0	1	0	1	1

Ограничения, определяющие очередность устранения обнаруженных уязвимостей, представлены в виде системы множеств $\Lambda=\{\lambda_j\}$ имеют вид:

$$\Lambda = \{\lambda_1 = \{2\}; \lambda_2 = \{\varnothing\}; \lambda_3 = \{\varnothing\}; \lambda_4 = \{\varnothing\};$$
$$\lambda_5 = \{1, 2, 6\}; \lambda_6 = \{\varnothing\}; \lambda_7 = \{4\}\}.$$

Решение задачи.

1. Этап формирования групп действий.

На основании матрицы контроля определяем перечень действий:

$$\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7, \varphi_8, \varphi_9, \varphi_{10}, \varphi_{11}, \varphi_{12}, \varphi_{13}, \varphi_{14}, \varphi_{15}, \varphi_{16}, \varphi_{17}, \varphi_{18}, \varphi_{19}$$

На основании ограничений Λ, определяющих очередность устранения уязвимостей для каждого i-го узла формируем группы действий b_{ik} и выстраиваем в них действия в порядке выполнения.

Таким образом, получаем следующие группы:

$$b_{11} = \{\varphi_2, \varphi_1, \varphi_4, \varphi_3\}; b_{12} = \{\varphi_5\}; b_{21} = \{\varphi_6\};$$
$$b_{31} = \{\varphi_7, \varphi_8\}; b_{32} = \{\varphi_9\}; b_{41} = \{\varphi_{10}\}; b_{42} = \{\varphi_{11}\};$$
$$b_{51} = \{\varphi_{12}\}; b_{52} = \{\varphi_{13}, \varphi_{15}\}; b_{53} = \{\varphi_{14}\};$$
$$b_{61} = \{\varphi_{16}, \varphi_{17}\}; b_{62} = \{\varphi_{18}\}; b_{63} = \{\varphi_{19}\}.$$

2. Этап формирования подпрограмм действий.

С помощью опроса экспертов были определены значения частных показателей для каждой из найденных уязвимостей:

g^1_1 = «отличная»; g^1_2 = «хорошая»;
g^1_3 = «удовлетворительная»;
g^2_1 = «удовлетворительная»;
g^2_2 = «удовлетворительная»;
g^2_3 = «удовлетворительная»;
g^3_1 = «удовлетворительная»;
g^3_2 = «отличная»;
g^3_3 = «средняя»;
g^4_1 = «отличная»;
g^4_2 = «удовлетворительная»;
g^4_3 = «удовлетворительная»;
g^5_1 = «удовлетворительная»;
g^5_2 = «отличная»;
g^5_3 = «удовлетворительная»;
g^6_1 = «удовлетворительная»;
g^6_2 = «удовлетворительная»;
g^6_3 = «средняя»;
g^7_1 = «хорошая»;
g^7_2 = «средняя»;
g^7_3 = «отличная».

Допустим, что экспертами первый показатель g^j_1, характеризующий j-ю уязвимость, определен как ОЧЕНЬ ВАЖНЫЙ. Второй показатель g^j_2 – как ВАЖНЫЙ, третий g^j_3 – НЕВАЖНЫЙ.

Найдем обобщенные показатели c_j для каждой уязвимости:

$$c_1 = g^1_1 * \varepsilon_1 + g^1_2 * \varepsilon_2 + g^1_3 * \varepsilon_3 = 1 * 0{,}5 + 0{,}75 * 0{,}3 + 0{,}25 * 0{,}2 = 0{,}5 + 0{,}225 + 0{,}05 = 0{,}775;$$
$$c_2 = g^2_1 * \varepsilon_1 + g^2_2 * \varepsilon_2 + g^2_3 * \varepsilon_3 = 0{,}25 * 0{,}5 + 0{,}25 * 0{,}3 + 0{,}25 * 0{,}2 = 0{,}5 + 0{,}225 + 0{,}05 = 0{,}25;$$
$$c_3 = g^3_1 * \varepsilon_1 + g^3_2 * \varepsilon_2 + g^3_3 * \varepsilon_3 = 0{,}25 * 0{,}5 + 1 * 0{,}3 + 0{,}25 * 0{,}2 = 0{,}5 + 0{,}225 + 0{,}05 = 0{,}525;$$
$$c_4 = g^4_1 * \varepsilon_1 + g^4_2 * \varepsilon_2 + g^4_3 * \varepsilon_3 = 1 * 0{,}5 + 0{,}25 * 0{,}3 + 0{,}5 * 0{,}2 = 0{,}5 + 0{,}225 + 0{,}05 = 0{,}675;$$
$$c_5 = g^5_1 * \varepsilon_1 + g^5_2 * \varepsilon_2 + g^5_3 * \varepsilon_3 = 0{,}25 * 0{,}5 + 1 * 0{,}3 + 0{,}25 * 0{,}2 = 0{,}5 + 0{,}225 + 0{,}05 = 0{,}475;$$
$$c_6 = g^6_1 * \varepsilon_1 + g^6_2 * \varepsilon_2 + g^6_3 * \varepsilon_3 = 0{,}25 * 0{,}5 + 0{,}25 * 0{,}3 + 0{,}5 * 0{,}2 = 0{,}5 + 0{,}225 + 0{,}05 = 0{,}3;$$
$$c_7 = g^7_1 * \varepsilon_1 + g^7_2 * \varepsilon_2 + g^7_3 * \varepsilon_3 = 0{,}75 * 0{,}5 + 0{,}5 * 0{,}3 + 1 * 0{,}2 = 0{,}5 + 0{,}225 + 0{,}05 = 0{,}725.$$

Вектор обобщенных показателей проверок будет иметь вид

$$C \equiv \{c_1 = 0{,}775; c_2 = 0{,}25; c_3 = 0{,}525; c_4 = 0{,}675; c_5 = 0{,}475; c_6 = 0{,}3; c_7 = 0{,}725\}.$$

С помощью метода термометра определим уровень значений обобщенных показателей уязвимостей (табл. 1):

Таблица 1

Значения уровней уязвимостей

уязвимость 1	уязвимость 2	уязвимость 3	уязвимость 4	уязвимость 5	уязвимость 6	уязвимость 7
Высокий	Низкий	Средний	Высокий	Средний	Низкий	Высокий

Для соблюдения требования необходимости устранения в первую очередь важных уязвимостей выполним анализ каждой группы на наличие действия, степень важности обобщенного показателя у которого выше, чем у действий следующих за ним. В случае нахождения такой группы создаём новую группу. В эту группу переносим действия, стоящие после действия с максимальным значением обобщенного показателя. Анализ показывает, что группы b_{11} и b_{31} имеют такие действия (φ_1 и φ_7). Поэтому вводим 2-е новые группы $\underline{b}_{13}$ и $\underline{b}_{33}$, в которые переносим действия, стоящие после действия с максимальным значением обобщенного показателя, получаем:

$$b_{11} = \{\varphi_2, \varphi_1\}; b_{12} = \{\varphi_5\}; \underline{b}_{13} = \{\varphi_4, \varphi_3\}; b_{21} = \{\varphi_6\};$$
$$b_{31} = \{\varphi_7\}; b_{32} = \{\varphi_9\}; \underline{b}_{33} = \{\varphi_8\}; b_{41} = \{\varphi_{10}\};$$
$$b_{42} = \{\varphi_{11}\}; b_{51} = \{\varphi_{12}\}; b_{52} = \{\varphi_{13}, \varphi_{15}\}; b_{53} = \{\varphi_{14}\};$$
$$b_{61} = \{\varphi_{16}, \varphi_{17}\}; b_{62} = \{\varphi_{18}\}; b_{63} = \{\varphi_{19}\}.$$

Используя правила (1) формируем из групп подпрограммы:

$$\Xi^B = \{b_{11}; b_{12}; b_{31}; b_{32}; b_{42}; b_{51}; b_{52}; b_{63}\};$$
$$\Xi^C = \{b_{13}; b_{21}; b_{33}; b_{41}; b_{61}; b_{62}\}; \Xi^H = \{b_{53}\}.$$

3. Этап формирования плана действий администратора.

Для каждого узла вычисляем значение коэффициента незащищенности:

$$s_1^{НЗ} = o_{11} \times c_1 + o_{12} \times c_2 + o_{13} \times c_3 + o_{14} \times c_4 + o_{15} \times c_5 + o_{16} \times c_6 + o_{17} \times c_7 =$$
$$= 1 \times 0{,}775 + 1 \times 0{,}25 + 0 \times 0{,}525 + 0 \times 0{,}675 + 1 \times 0{,}475 + 1 \times 0{,}3 + 1 \times 0{,}725 = 2{,}525;$$

$$s_2^{НЗ} = o_{21} \times c_1 + o_{22} \times c_2 + o_{23} \times c_3 + o_{24} \times c_4 + o_{25} \times c_5 + o_{26} \times c_6 + o_{27} \times c_7 =$$
$$= 0 \times 0{,}775 + 0 \times 0{,}25 + 1 \times 0{,}525 + 0 \times 0{,}675 + 0 \times 0{,}475 + 0 \times 0{,}3 + 0 \times 0{,}725 = 0{,}525;$$

$$s_3^{НЗ} = o_{31} \times c_1 + o_{32} \times c_2 + o_{33} \times c_3 + o_{34} \times c_4 + o_{35} \times c_5 + o_{36} \times c_6 + o_{37} \times c_7 =$$
$$= 1 \times 0{,}775 + 0 \times 0{,}25 + 0 \times 0{,}525 + 0 \times 0{,}675 + 1 \times 0{,}475 + 0 \times 0{,}3 + 1 \times 0{,}725 = 1{,}975;$$

$$s_4^{НЗ} = o_{41} \times c_1 + o_{42} \times c_2 + o_{43} \times c_3 + o_{44} \times c_4 + o_{45} \times c_5 + o_{46} \times c_6 + o_{47} \times c_7 =$$
$$= 0 \times 0{,}775 + 0 \times 0{,}25 + 1 \times 0{,}525 + 1 \times 0{,}675 + 0 \times 0{,}475 + 0 \times 0{,}3 + 0 \times 0{,}725 = 1{,}2;$$

$$s_5^{НЗ} = o_{51} \times c_1 + o_{52} \times c_2 + o_{53} \times c_3 + o_{54} \times c_4 + o_{55} \times c_5 + o_{56} \times c_6 + o_{57} \times c_7 =$$
$$= 1 \times 0{,}775 + 0 \times 0{,}25 + 0 \times 0{,}525 + 1 \times 0{,}675 + 0 \times 0{,}475 + 1 \times 0{,}3 + 1 \times 0{,}725 = 2{,}475;$$

$$s_6^{НЗ} = o_{61} \times c_1 + o_{62} \times c_2 + o_{63} \times c_3 + o_{64} \times c_4 + o_{65} \times c_5 + o_{66} \times c_6 + o_{67} \times c_7 =$$
$$= 0 \times 0{,}775 + 1 \times 0{,}25 + 1 \times 0{,}525 + 0 \times 0{,}675 + 1 \times 0{,}475 + 0 \times 0{,}3 + 1 \times 0{,}725 = 1{,}975;$$

$$S^{НЗ} = \{ s_1^{НЗ} = 2{,}525;\ s_2^{НЗ} = 0{,}525;\ s_3^{НЗ} = 1{,}975;\ s_4^{НЗ} = 1{,}2;\ s_5^{НЗ} = 2{,}475;\ s_6^{НЗ} = 1{,}975\}.$$

Для каждой группы вычисляем значение среднего обобщенного показателя группы:

$v_{11} = 0{,}51$; $v_{12} = 0{,}72$; $v_{31} = 0{,}77$; $v_{32} = 0{,}72$; $v_{42} = 0{,}67$;
$v_{51} = 0{,}77$; $v_{52} = 0{,}7$; $v_{63} = 0{,}72$; $v_{13} = 0{,}6$; $v_{21} = 0{,}52$;
$v_{33} = 0{,}47$; $v_{41} = 0{,}52$; $v_{61} = 0{,}387$; $v_{62} = 0{,}47$; $v_{53} = 0{,}3$.

Зная значения среднего обобщенного показателя каждой группы, рассчитываем мультипликативный показатель:

$u_{11} = 1{,}29$; $u_{12} = 1{,}83$; $u_{31} = 1{,}53$; $u_{32} = 1{,}43$; $u_{42} = 0{,}81$;
$u_{51} = 1{,}92$; $u_{52} = 1{,}73$; $u_{63} = 1{,}43$; $u_{13} = 1{,}52$; $u_{21} = 0{,}28$;
$u_{33} = 0{,}94$; $u_{41} = 0{,}63$; $u_{61} = 0{,}77$; $u_{62} = 0{,}94$; $u_{53} = 0{,}74$.

Значение мультипликативного показателя является критерием для упорядочивания групп действий в подпрограммах. Упорядочивание производится прямым методом ранжирования:

$$\Xi^B = \{ b_{51}; b_{12}; b_{52}; b_{31}; b_{32}; b_{63}; b_{11}; b_{42} \};$$
$$\Xi^C = \{b_{13}; b_{33}; b_{62}; b_{61}; b_{41}; b_{21}\};\ \Xi^H = \{b_{53}\}.$$

Формирование плана действий администратора производится при помощи жадного алгоритма выбора порядка действий. В первую очередь в план действий включаются действия групп из подпрограммы с высоким уровнем обобщенного показателя, далее из подпрограммы со средним уровнем обобщенного показателя, а потом из подпрограммы с низким уровнем:

$$\Phi = \{\varphi_{12}, \varphi_5, \varphi_{13}, \varphi_{15}, \varphi_7, \varphi_9, \varphi_{19}, \varphi_2, \varphi_1, \varphi_{11}, \varphi_4, \varphi_3, \varphi_8, \varphi_{18}, \varphi_{16}, \varphi_{17}, \varphi_{10}, \varphi_6, \varphi_{14}\}.$$

План действий администратора безопасности показывает последовательность действий, которые необходимо выполнить администратору для устранения обнаруженных уязвимостей.

Выводы

В статье представлена методика формирования плана действий администратора безопасности компьютерной сети по результатам проведенного контроля защищенности. Данная методика обеспечивает уменьшение работного времени администратора и повышает оперативность принятия решения администратором за счет автоматического выполнения этапа информационной подготовки принятия решения по повышению уровня защищенности компьютерной сети. Это позволяет, как показали результаты исследований, сократить на 8 – 12% общее время затрачиваемое администратором на проведение мероприятий по обеспечению повышения уровня защищенности компьютерной сети до требуемого уровня.

Список литературы

1. Шохін Б.П., Юдін О.М., Мазулевський О.Є. Вдосконалення контролю за станом захищеності комп'ютерної мережі на основі адаптивного моніторингу // Зб. наук. пр. ВІТІ НТУУ «КПІ» – К.: НТУУ «КПІ». – 2004. – № 4. – С. 208-217.

2. Герасимов Б.М., Тарасов В.А., Токарев И.В. Человеко-машинные системы. Принятие решений с элементами искусственного интеллекта. – К.: Наук. думка, 1993. – 184 с.

3. Теория расписаний и вычислительной машины / Под ред. Э.Г. Кофмана. – М.: Наука, 1984. – 333 с.

4. Безгинов А.Н., Трегубов С.Ю. Обзор существующих методов составления расписаний // Информационные технологии и программирование: Межвузовский сборник статей. – М.: МГИУ. – 2005. – № 2 (14). – С. 5-18.

5. Тим Джонс М. Программирование искусственного интеллекта в приложениях. – М.: ДМК Пресс, 2004. – 312 с.

6. Герасимов Б.М., Дивизинюк М.М., Субач И.Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. – Севастополь: Издательский центр СНИЯЭиП, 2004. – 320 с.

7. Новиков Ф.А. Дискретная математика для программистов. – СПб.: Питер, 2000. – 304 с.

8. Свами М., Тхуласираман К. Графы, сети и алгоритмы. – М.: Мир, 1984. – 455 с.

9. Анохин А.М., Глотов В.А., Павельев В.В., Черкашин А.М. Методы определения коэффициентов важности критериев // Автоматика и телемеханика. – 1997. – № 8. – С. 3-35.

Поступила в редакцию 1.08.2006

Рецензент: д-р техн. наук, проф. Р.Г. Савенко, Полтавский национальный технический университет, Полтава.