УДК 004.056.53

Понятие компрометирующей информации в общей схеме анализа уязвимости автоматизированных систем

Шемяков А. О.

Московский авиационный институт (национальный исследовательский университет), МАИ, Волоколамское шоссе, 4, Москва, А-80, ГСП-3, 125993, Россия

e-mail: a.shemyakov@gmail.com

Аннотация

В статье раскрывается понятие компрометирующей информации, рассматриваются варианты интерпретации включения в информацию о системе компрометирующей ее информации. Для каждого случая оценивается уязвимость системы.

Ключевые слова

автоматизированная система, уязвимость системы, компрометирующая информация, информационное поле, энтропия

При исследовании автоматизированной системы (АС) на предмет оценки ее уязвимости, возникает необходимость включения в этот процесс понятия компрометирующей информации *Ci*. «Прикладные» аспекты этого понятия в общей схеме анализа уязвимости АС рассмотрены в настоящей работе.

Различные варианты включения в общую информацию об АС компрометирующей ее информации *Ci*, со всеми необходимыми комментариями представлены на рисунке 1.

Соотношение объемов общей I_S информации о системе и *Ci* могут быть самыми различными. При этом, с учетом определения уязвимости АС, больший объем информации *Ci* не всегда будет означать бóльшую уязвимость.

Если, например, в исследуемой системе *Ci* сконцентрирована (локализована) в информационном поле одного из элементов (вариант 1), и нарушитель не знает об этом, то для выявления ее уязвимости он должен будет получить информацию обо всех *N* элементах АС (данное утверждение пока не учитывает информационную зависимость элементов АС). Начальная неопределенность $H_н$ или мера незнания нарушителем такой АС будет равнозначна

неопределенности системы, в которой *Ci* распределена в информации о каждом элементе (вариант 2) и может быть оценена зависимостью:

$$H_{н}^{(1)} = H_{н}^{(2)} = -\sum_{j=1}^{2^N} p_j \log_2 p_j \,, \qquad (1)$$

где p_j – априорная вероятность осведомленности нарушителя о *j*-й комбинации элементов АС ($j = 1,2,\ldots, 2^N$).

Если в результате предварительных исследований информационного поля АС и ВС им получена информация об *n* элементах, то неопределенность АС снижается до уровня:

$$H_{н}^{(1)*} = H_{н}^{(2)*} = -\sum_{j=1}^{2^{N-n}} p_j \log_2 p_j \,. \qquad (2)$$

Однако вероятность выявления такой уязвимости за определенное время (при условии, что время дискретно и на каждом временном шаге нарушитель получает информацию только об одном элементе) будет различной для первого и второго варианта распределения *Ci*.

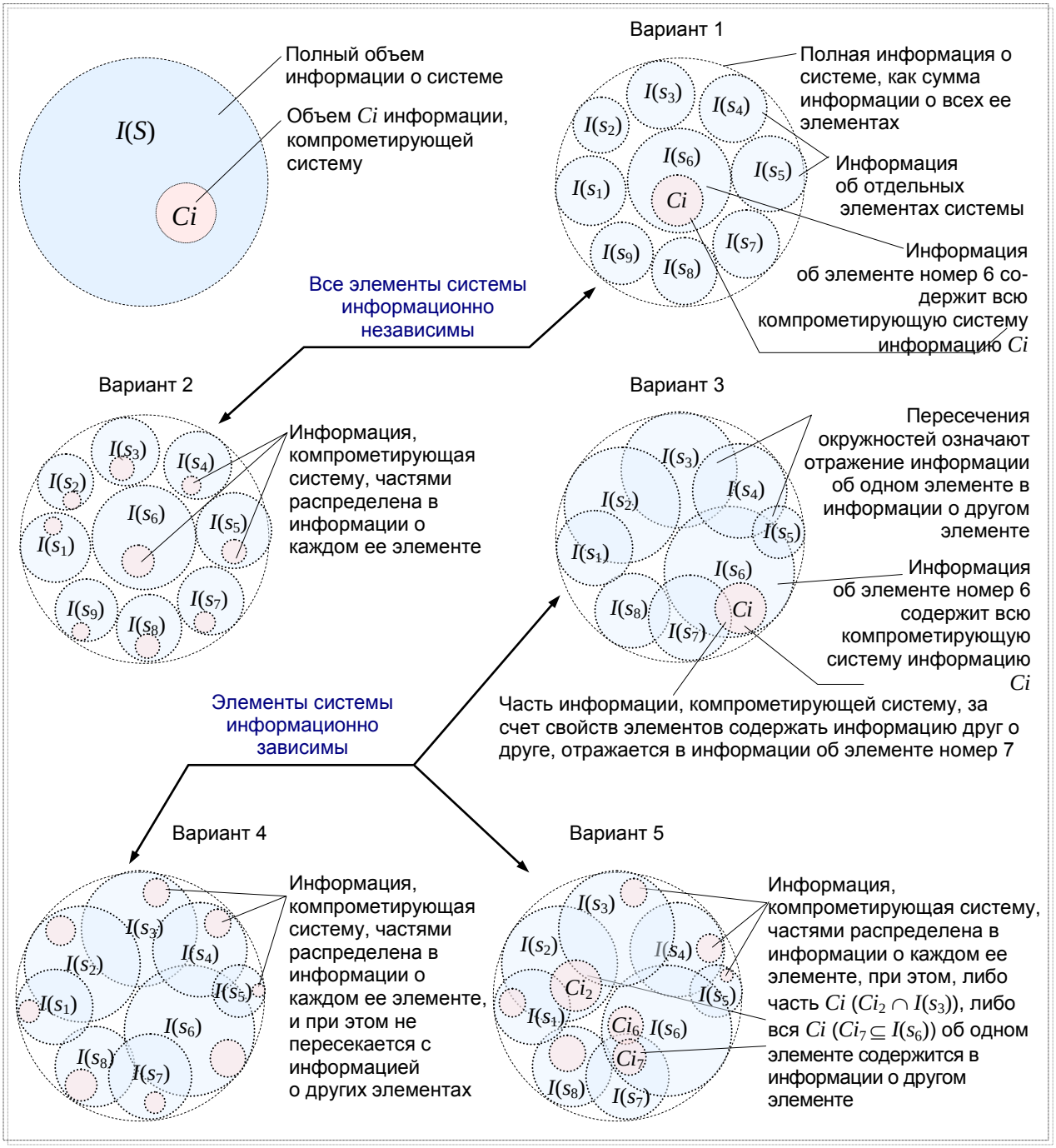

Рис. 1. Различные варианты графической интерпретации включения в информацию о системе компрометирующей ее информации *Ci*

Для первого варианта распределения *Ci* вероятность Q_k выявления уязвимости АС за r шагов будет определяться отношением:

$$Q_r^{(1)} = \frac{1}{N - r + 1}, \qquad (3)$$

а для второго варианта:

$$Q_r^{(2)} = \begin{cases} 0, & \text{при } r < N \\ 1, & \text{при } r = N \end{cases}. \qquad (4)$$

Таким образом, если не учитывать информационную взаимосвязность элементов АС, то вероятность ее компрометации на интервале времени от 0 до t_r ($r < N$) при рассмотрении первого варианта распределения *Ci* будет всегда выше. Это прямое следствие из сравнения (3) и (4). Косвенное, состоит в том, что математическое ожидание «трудозатрат» нарушителя на выявление уязвимости АС при рассмотрении второго варианта распределения *Ci* будет большим по сравнению с первым вариантом.

На случай информационной взаимосвязности элементов АС (см. рисунок варианты 3, 4 и 5), рассмотренные выше следствия не действительны. Причина этого лежит в том, что, либо часть, либо вся *Ci* об одном элементе может содержаться в информации о другом элементе. Поэтому при получении нарушителем доступа к информации I_k об элементе s_k существует отличная от нуля вероятность получения им на основании нее компрометирующей информации Ci_m об элементе s_m.

Рассматривается пересечение информации двух элементов: I_m и I_k в объемах информации i_m и i_k соответственно, см. рисунок 2.

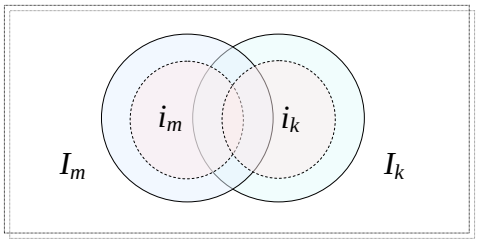

Рис. 2. Пересечение информационных фрагментов I_m и I_k

Вероятность того, что информация I_m будет известна в объеме i_m: $I_m = i_m$, при условии, что информация I_k известна в объеме i_k: $I_k = i_k$, - записывается как $p(i_m|i_k)$. Условная энтропия $H_{m|k}$ определяется как [0,2]:

$$H_{m|k} = -\sum_{i_k} p(i_k) \sum_{i_m} p(i_m | i_k) \log p(i_m | i_k) = -\sum_{i_k} \sum_{i_m} p(i_k, i_m) \log p(i_m | i_k). \qquad (5)$$

В выражении (5) величина $p(i_k,i_m)$ определяет вероятность событий $I_k = i_k$ и $I_m = i_m$.

Энтропия $H_{m|k}$ характеризует степень неопределенности элемента s_m, оставшуюся после того, как состояние элемента s_k полностью определимость и является мерой усредненного количества информации, содержащегося в информации I_m, если известна информация I_k. При этом необходимо заметить, что неравенство $H_{m|k} \le H_m$ выполняется

всегда (док-во см. [2], с. 70), а неравенство $H_{m|k} \neq H_{k|m}$ – в большинстве случаев [1]. В частности это имеет место быть, когда между i_k (или I_k) и i_m (или I_m) имеется зависимость, но односторонняя: например, информация об элементе s_m в объеме i_m (или I_m) полностью определяет информацию об элементе s_k в объеме i_k (или I_k), но не наоборот. В этом случае $H_{k|m} = 0$, а $H_{m|k} > 0$.

Понятие условной энтропии в данном случае необходимо для перехода к следующей величине: полному количеству информации, определяемому как:

$$I(s_k : s_m) = \sum_{i_k} \sum_{i_m} p(i_k, i_m) \log \frac{p(i_k, i_m)}{p(i_k) p(i_m)} = H_k - H_{k|m}. \qquad (6)$$

По определению, величина $I(s_k : s_m)$ есть мера количества информации, содержащейся в величинах I_k и I_m друг относительно друга. Если величины I_k и I_m являются независимыми, то $p(i_k,i_m) = p(i_k)p(i_m)$ и, следовательно, величина $I(s_k : s_m) = 0$. Если эта зависимость односторонняя (например, как в рассмотренном выше примере), то $I(s_k : s_m) = H_k$.

Зависимости между основными мерами информации показаны на рисунке 3.

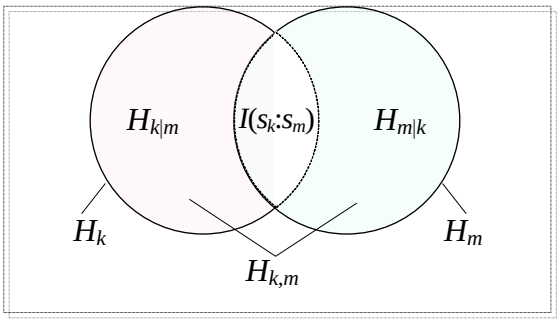

Рис. 3. Графическая интерпретация зависимостей между мерами информации

То, что $I(s_k : s_m)$ одинаковым образом зависит как от I_k, так и от I_m [2], говорит, что количество информации является не характеристикой одного из этих фрагментов, а характеристикой их связи, характеристикой соответствия состояний неопределенности элементов s_k и s_m.

В самом общем случае величина $I(s_k : s_m)$ определяет в какой мере знание состояния элемента s_m определяет состояние элемента s_k. Неравенство $I(s_k : s_m) \neq 0$ означает наличие информационной зависимости между элементами s_k и s_m. Эта связь существует, если один элемент содержит какую-либо информацию о другом элементе.

Таким образом, в случае информационной взаимосвязности элементов АС нарушитель, получая доступ к одному из них, «автоматически» может получить

информацию обо всех с ним связанных элементах в том объеме, в котором она содержится в этом элементе.

Проблемным в данном случае остается вопрос о распределении *Ci* по элементам АС. Ответ на него можно было бы получить, если бы имелась возможность формальной идентификации «содержимого» I_m с *Ci* по каким-либо существенным признакам. Однако, несмотря на ранее сформулированное определение понятия компрометирующей информации, реально провести такую идентификацию практически невозможно. В большинстве случаев, предсказать какую информацию и посредством чего нарушитель инвертирует в *Ci*, заранее не возможно. Это не формализуемая творческая деятельность человека. Любая методика здесь будет носить условный характер, определяя априори лишь некие правила, по которым должен мыслить и действовать нарушитель.

Необходимо также отметить, что в качестве исходной точки для выявления уязвимости всей системы, нарушителем может быть выбран элемент, на который эксперт может и не обратить внимания.

В связи с этим, при исследовании уязвимости АС, предлагается принять следующее определение компрометирующей информации: информация Ci_m, компрометирующая элемент s_m – уникальное отображение информации об этом элементе I_m на множество $\left\{E_m^{Ci}\right\}$ таких его состояний, при которых возникает реально предсказуемая возможность нарушения способности выполнения присущей ему локальной функции:

$$Ci_m : I_m \to \left\{E_m^{Ci}\right\},\ \left\{E_m^{Ci}\right\} \cup \left\{E_m^{n}\right\} = \varnothing \qquad (7)$$

где $\left\{E_m^{n}\right\}$ – множество состояний элемента s_m, при которых возможно выполнения присущей ему локальной функции.

Так как каждый элемент в АС выполняет какую-то функцию (в противном случае он бы просто не был включен в состав АС), то при анализе ее уязвимости принимается во внимание следующее допущение, что компрометирующая АС информация *Ci*, содержится во всех N ее элементах. При этом акцент ставится не на объеме Ci_m, а степени ее значимости для уязвимости АС. В свою очередь степень значимости Ci_m, включаемой в I_m элемента-ТЭ определяется важностью для функционирования АС осуществляемых им преобразований входов в выходы других элементов, а в случае I_m элемента-НИ – фактом содержания в нем информации об s_k-ом элементе-ТЭ с соответствующей степенью значимости его Ci_k.

С учетом принятого допущения, исследование уязвимости любой АС должно проводиться относительно каждого ее s_m элемента в контексте присущей ему $A_{h,m}$ совокупности отношений преобразований и связей с другими элементами АС.

Таким образом, существенным моментом при оценке степени значимости Ci_m и последующей декомпозиции исходного множества элементов АС на подмножества M_i^z и M_1^z является схема связей ее элементов, априори выступающих в роли проводников угрозы безопасности.

Библиографический список

1. Стин Э. Квантовые вычисления. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2000, 112 с.

2. Тарасенко Ф.П. Введение в курс теории информации. – Томск: Издательство Томского университета, 1968. – 240 с.