УДК 004.8

О ПРИМЕНЕНИИ ПРИНЦИПА ЛОКАЛИЗАЦИИ ПРИ ОЦЕНКЕ ЭФФЕКТИВНОСТИ МОДЕЛЕЙ КОНТРОЛЯ ЗАЩИЩЕННОСТИ СИСТЕМ

А.Ю. Максимовский
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: maximay@ipu.ru

Ключевые слова: оценка защищенности информационных систем, аудит безопасности.

Аннотация: В докладе рассмотрен ряд аспектов использования принципа локализации для построения и оценки эффективности непротиворечивой аддитивной ролевая модели контроля защищенности, предполагающая совместное применение подсистемы внутреннего контроля (ПВК) системы и внешнего аудита для широкого класса информационных систем. Разработаны рекомендации по выбору параметров (характеристик) (ПВК) и внешнего аудита, а также по оптимизации работ по поддержанию безопасного функционирования системы.

1. Введение

Оценка защищенности информационной системы является одной из важнейших задач на протяжении всего жизненного цикла ее существования от этапа разработки до утилизации. Принципы и методики оценивания могут отличаться в зависимости из целей, условий и этапа функционирования системы. Применительно к системам, относящимся к критической информационной инфраструктуре (далее – КИИ), в работах [1-3] предложены подходы к построению параметрических моделей оценки уровня информационной безопасности и рискового потенциала КИИ. Вместе с тем, в ряде практических случаев необходимы, с одной стороны, менее «глобальные» подходы, потому что уровень и объем угроз не сопоставимы с КИИ, и, с другой стороны, нужны определённые гарантии по оперативности восстановления работоспособности системы, если ее текущее состояние представляется небезопасным. В докладе рассмотрены ряд аспектов применения принципа локализации для решения этих задач в рамках нелинейной аддитивной ролевой модели контроля защищенности, предполагающей совместное применение подсистемы внутреннего контроля системы и внешнего аудита.

2. Модель оценки защищенности системы

Пусть C – некоторая система, содержащая N элементов. Предполагается, что система C функционирует в определенном временном пространстве. Дискретность или

непрерывность времени не являются существенными. Каждый элемент e_i имеет идентификатор $i, 1 \le i \le N,$ и характеризуется состоянием $s(i,t)$ в момент времени (такт работы системы) *t.*

Состояния $s(i,t)$ элементов e_i принимают значения из действительного числового интервала [0,1], при этом $s(i,t) = 0$, если элемент e_i не функционирует в момент *t*. Полагаем, что система *C* безопасно функционирует момент времени *t*, если выполнено

(1) $S_C(t) = \sum_{i=1}^{N} s(i,t) \le 1.$

Роли участников процедуры присвоены оценок состояния $s(i,t)$ элемента e_i, описываются следующим образом.

1) Подсистема внутреннего контроля системы (ПВК) присваивает элемента e_i оценку состояния $\mathrm{c}(i,t)$, которая принимает одно из *r* значений $0 \le c_1 < c_2 <..< c_r \le 1$. При этом запись $\mathrm{c}(i,t) = 0$ означает, что элемент e_i и его текущие настройки полностью соответствуют конструкторской документации.

2) Аудитор присваивает элементу e_i оценку $d(i,t)$, принимающую одно из k действительных значений $0 \le d_1 < d_2 <..< d_k = 1$. При этом допускается, что значение $\mathrm{c}(i,t)$ не может быть меньше оценки $d(i,t)$, то есть оценка аудитора «строже» результата, полученного ПВК, и значения состояния, установленного при старте системы или простое элемента. Такая ситуация часто реализуется на практике. В частности, если $s(i,t) = d_k$, то элемент e_i непригоден к дальнейшей эксплуатации в текущем состоянии.

3) Текущие состояния $s(i,t)$ элементов e_i, которые в соответствии с (1), позволяют оценить безопасность функционирования системы в целом, с учетом пунктами 1,2, вычисляется как сумма двух оценок $s(i,t) = c(i,t) + d(i,t)$.

Тем самым достигается непротиворечивость результатов ПВК и аудита в случае их одновременного проведения. При этом оценка безопасности функционирования системы является не линейной функцией ввиду условия $c(i,t) \le d(i,t)$.

Без ограничения общности будем считать, что оценка действий персонала (пользователей) системы включается в оценки ПВК и Аудитора.

4) Администратор системы в начальный момент времени (для простоты, *t*=0) присваивает всем состояниям значение $s(i,0) = 0, 1 \le i \le N,$. Кроме того, Администратор также может присвоить значение $s(i,t) = 0$, если в момент времени *t* элемент e_i и его настройки полностью соответствуют эксплуатационной документации. Это соответствует ситуации, когда Администратор имеет гарантии, что функционирование данного элемента соответствует требованиям эксплуатационной документации или элемент не функционирует.

3. Вероятностная модель процедуры оценки защищенности системы

Определим вероятностную модель присвоения значений состояний $s(i,t)$.

1) ПВК присваивает элементу e_i оценку состояния $c(i,t)$ случайно в соответствии с некоторым распределением вероятностей $P(c(i,t) = c_g) = p_g$. При этом данное распределение не зависит ни от индекса *i*, ни от момента времени *t*.. Обозначим γ случайную величину, принимающую значение c_g из множества $\{c_1, c_2, \dots, c_r\}$ с вероятностью p_g.

Сделаем ряд замечаний о моментах случайной величины γ. Математическое ожидание E=Eγ случайной величины γ, равное $E = \sum c_g p_g$, очевидно, в соответствии с условием $0 \le c_1 < c_2 <..< c_r \le 1$, не превосходит 1. Для исключения тривиального

случая будем полагать, что $E > 0$. С другой стороны, выполнение условия (1) означает, что $NE \leq 1$. Таким образом, по данным, полученным ПВК, работоспособными окажутся, в среднем, $N(1\text{-}E)$ элементов системы, что допустимо, если эта величина близка к *N*. Степень такой близости, характеризуемая величиной $\varepsilon = (1\text{-}E)$, может рассматриваться как один из параметров настройки ПВК. В отношении дисперсии Dγ случайной величины γ с учетом $(c_g)^2 \leq c_g, E \neq 0$, справедливы оценки $0 < D\gamma \leq 1$.

Замечание 1. Данные оценки не только характеризуют точность результатов ПВК, но и представляет интерес для расширения обсуждаемой модели на случай, когда распределения вероятностей $P(c(i,t) = c_g) = p_g$, различны для разных элементов e_i и вектор значений $c_1 < c_2 <..< c_r$ фиксирован. В этом случае при достаточно большом числе *N* элементов системы выполнены условия Линдеберга (см. [4, с. 354]) для нормальной аппроксимация распределения данных ПВК $V_C(t) = \sum c(i,t)$.

Замечание 2. Функция $V_C(t)$ показывает «локальный вклад» ПВК в значение $S_C(t)$ и может служить показателем «внутренней» защищенности системы *C*..

В данной модели при разработке ПВК и настройке ее параметров целесообразно:

1) разработать перечень состояний элементов системы (при необходимости, для каждого элемента), упорядоченный по степени критичности (с точки зрения безопасности функционирования элемента и системы в целом), и присвоить каждому состоянию элемента показатель из множества $\{c_1, c_2, \dots, c_r\}$, $0 \leq c_1 < c_2 <..< c_r \leq 1$;

2) определить приемлемые с эксплуатационной точки зрения значения параметров $\varepsilon = (1\text{-}E)$ и, соответственно, $P(c(i) = c_g) = p_g$;

3) в ходе эксплуатации уточнять параметры $\{c_1, c_2, \dots, c_r\}$, и $P(c(i) = c_g) = p_g$;

4) проводить корректировку параметров $\{c_1, c_2, \dots, c_r\}$, и $P(c(i) = c_g) = p_g$;

Пункт 4) отражает ситуацию, когда в ходе аудита были обнаружены некорректные или неактуальные настройки параметров ПВК.

5) Оценка $d((i,t)$, присваиваемая Аудитором элементу e_i, характеризует, в основном, добросовестность пользователя элемента. Поэтому воспользоваться вероятностной моделью ПВК можно с поправкой, что в качестве вероятностей $P(d(i,t) = d_g) = q_g$ выступают оценки этих показателей, основанные на фактических данных аудиторских проверок. Обозначим δ случайную величину, принимающую значение d_g из множества $\{d_1, d_2, \dots, d_k\}$ с вероятностью q_g. Будем считать, что в фиксированный момент времени *t* распределение этой случайной величины не зависит от индекса *i*. Случайные величины γ и δ при условии «строгости аудита» они являются зависимыми.

Обозначим Δ математическое ожидание случайной величины δ. Очевидно, $\Delta \leq 1$. Для исключения тривиального случая также будем полагать, что $\Delta > 0$. При этом аналогично предыдущему $0 < D\delta \leq 1$.

Замечание 3. Аддитивность функции $S_C(t)$ позволяет по аналогии с функцией $V_C(t)$ определить функцию $A_C(t) = S_C(t) - V_C(t) = \sum_{i=1}^{N} d(i,t) \leq 1$., которая показывает «вклад» Аудитора в значение$S_C(t)$ и может служить показателем значимости вклада «внешнего» контроля в оценку защищенности системы *C* в момент времени *t*.

Для организации действий Аудитора в рамках данной модели целесообразно:

1) разработать перечень показателей (оценок) состояний элементов системы (при необходимости, для каждого элемента), и присвоить каждому состоянию элемента показатель из множества $\{d_1, d_2, \dots, d_k\}$, $0 \leq d_1 \dots < d_k \leq 1$;

2) оценить на основании фактических результатов аудита однотипных систем и их элементов значения вероятностей $P(d(i) = d_g) = q_g$;

3) на основании опыта практического применения корректировать параметры

$d_1, d_2, \dots, d_k$ и вероятности $P(d(i) = d_g) = q_g$;;

4) дополнить условием «строгости аудита»: для любых i и t $c((i,t) \le d((i,t)$, процедуру присвоения оценок состояниям $s(i,t) = c((i,t) + d((i,t)$.

Оценим среднее и дисперсию значения функции $S_C(t)$. Стандартными методами вычисляя среднего и дисперсии случайной величины $\sigma(i,t) = \gamma(i,t) + \delta(i,t)$,, равной состоянию $s(i,t)$, несложно убедиться в справедливости оценок:

- $0 < E\sigma(i,t) = E + \Delta \le 2$
- $D\sigma(i,t) \le E + 3\Delta - E^2 - 2E\Delta - \Delta^2 = E(1- E - 2\Delta) + \Delta(3 - \Delta) = D^*$.

Поэтому среднее и дисперсия значения функции $S_C(t)$ находятся в пределах от 0 до ND^*. При этом если за счет настройки параметров ПКВ можно обеспечить выполнение неравенства для среднего значения функции $V_C(t) \le 1$, то для достижения выполнения условия для среднего значения функции $S_C(t) \le 1$ в условиях «строгости аудита» необходимо тщательное исполнение требований Аудитора. Данное обстоятельство важно при выборе параметров $d_1, d_2, \dots, d_k$ с учетом оценок соответствующих значениях вероятностей $q_1, q_2, \dots, q_k$.

Вероятность $P(t)$ безопасного функционирования системы C в момент времени t представима в виде произведения

$P(t) = P(\sum_i \sigma(i,t) \le 1) = P(\sum_i \gamma(i,t) \le 1)\, P(\sum_i \delta(i,t) \le (1 - \sum_i \gamma(i,t))$.

Если $V_C(t) \le 1$, то из условии $\gamma(i,t) \le \delta(i,t)$ получаем, что

$$P(t) = P(\sum_i (\delta(i,t) - \gamma(i,t)) \ge 1 - V_C(t)) .$$

Тем самым в рамках рассматриваемой модели мы получили еще одну оценку степени влияния Аудитора на оценку безопасности функционирования системы.

4. Применение принципа локализации для оптимизации работ по восстановлению безопасного функционирования системы

Рассмотрим вопрос оптимизации восстановления безопасного функционированием системы C в рамках описанной модели с точки зрения выполнения системой в целом или ее компонентами своих функциональных задач, используя в качестве метрики ущерб (временные издержки) функциональности, возникающий при необходимости прекращать использование отдельных элементов системы при условии $S_C(t) \ge 1$

Рассмотрим двух базовых сценария действий Администратора системы:

1) в случае $S_C(t) \ge 1$ система останавливается, и в течение некоторого времени τ проводятся работы по приведению всех элементов $e_i, 1 \le i \le n$, системы в безопасное состояние, чтобы обеспечить или выполнение условия $s(i, t+\tau) = 0$, где $1 \le i \le n$, или, реализации условия (1) для $S_C(t+\tau)$. При этом затраты пропорциональны величине τN;

2) в системе C выделяется подсистема C', состоящая из элементов с индексами $\{j_1, \dots, j_m(t)\}$, сумма состояний которых $S_{C'}(t) = \sum s(j(l), t) \le 1$, и осуществляется временная эксплуатация подсистемы C', пока не будут возвращены в требуемое (или допустимое в соответствии с условием (1)) состояния остальные элементы. В частности, в качестве такой подсистемы C' может выступать резервная подсистема системы C.

Очевидно, второй сценарий является более предпочтительным – при временной потере $N\text{-}m(t)$ элементов затраты на восстановление работоспособности системы становятся пропорциональны величине $\tau(N\text{-}m(t))$.

Будем считать, что время $\tau(s(i,t)/s'(i,t')) = t' - t$, необходимое для снижения оценки $s(i,t) = c(i,t) + d(i,t)$ до оценки $s'(i,t') = c'(i,t')) + d'(i,t')$, соответственно, $(\tau((c((i,t)/c'((i,t'))$, $\tau((d((i,t)/d'((i,t')))$, пропорционально разностям

$c(i,t)$ - $c'((i,t')$ и $d(i,t)$ - $d'((i,t')$ с коэффициентами α и β соответственно.

Тогда если $S_C(t) \geq 1$ и $S_C(t') \leq 1$, то время $t_{восст}$, требуемое для восстановления безопасного функционирования системы C, вычисляется по формуле

$$t_{\text{восст}} = t'\,t = \max_i \alpha(c'(i,t') - c((i,t)) + \max_i \beta(d'(i,t') - d(i,t)).$$

Эта формула позволяет получить условие для нижней границы $t_{\text{ауд}}$ проведения очередного аудита, а именно $t_{\text{восст}} \leq t_{\text{ауд}}$, а также наметить путь оптимизации действий Администратора путем поиска в системе С подсистем C', элементы которых с индексами $\{j_1, \dots, j_{m(t)}\}$ не только удовлетворяют неравенству $S_{C'}(t) = \sum s(j(l),t) \leq 1$, но и величина $t_{\text{восст}}(C \backslash C')$ минимальна.

Замечание 5. Для определения функционалов с помощью формул вида (1) достаточно, чтобы значения $c_1, c_2, \dots, c_r$ и $d_1, d_2, \dots, d_k$ принадлежали частично упорядоченной абелевой группе, что открывает потенциальную возможность использовать в качестве таких значений векторы из векторных пространств с подходящей метрикой. Поэтому представляет значительный интерес исследование алгебраических моделей, применяемых для описания и обоснования адекватности решающих правил контроля защищенности информационных систем.

5. Заключение

На основе принципа локализации в докладе:

- предложена непротиворечивая аддитивная ролевая модель контроля защищенности произвольной системы, предполагающая применение подсистемы внутреннего контроля (ПВК) системы и внешнего аудита;
- разработаны рекомендации по выбору параметров (характеристик) (ПВК) и внешнего аудита, а также по оптимизации работ по поддержанию безопасного функционирования системы;
- найдены условия асимптотической нормальности распределения значений функции, характеризующей степень защищенности системы, что позволяет расширить градацию степеней защищенности системы, используя подходящие квантили распределения значений указанной функции.

Список литературы

1. Калашников А.О., Аникина Е.В. Метод эффективного распределения сканеров для мониторинга информационной безопасности узлов гетерогенной сети // Информация и безопасность. 2018. Т. 21, Вып. 4. С. 455-464.
2. Калашников А.О., Аникина Е.В. Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний(часть2) // Информация и безопасность. 2018. Т. 21, Вып.2. С. 155-164.
3. Калашников А.О., Сакрутина Е.А. Модель прогнозирования рискового потенциала значимых объектов критической информационной инфраструктуры // Информация и безопасность. 2018. Т. 21, Вып. 4. С. 465-470.
4. Ширяев А.Н. Вероятность, 1980, М.: Наука, 576 с.