УДК 681.324

АЛГУЛИЕВ Р.М.

ОБ ОДНОЙ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ФУНКЦИОНИРОВАНИЯ АДМИНИСТРАТОРА БЕЗАПОСНОСТИ ГИПОТЕТИЧЕСКОЙ КОМПЬЮТЕРНОЙ СЕТИ ПРИ БОРЬБЕ С УГРОЗАМИ

Предположим, что какая-нибудь гипотетическая компьютерная сеть, требующая решение вопросов информационной безопасности в рамках единой политики безопасности разбита на f областей (например, intranet, LAN и т.д.), $f = \overline{1,F}$. В каждой области необходимо осуществит защиту r_f ресурсов (сервера, маршрутизаторы, По, файлы и т.д.), $r_f = \overline{1,R_f}$, $f = \overline{1,F}$. Допустим, что в целях выполнения комплексных задач информационной безопасности компьютерной сети выделен самостоятельно функционирующий администратор безопасности (АБ). Известно, что одной из главных функций АБ является своевременное принятие решений при наличии разноприродных угроз к защищаемым ресурсам. Для выполнения этой функции в распоряжении АБ имеется определенное множество $Z = \left\{ z_i \middle| i = \overline{1,I} \right\}$ механизмов защиты от угроз. Кроме того, на каждую защищаемую область f назначен регистратор событий e_f, в функцию которого входит сбор информацию о наличии угроз к ресурсам r_f, определение вида и количества угроз и оперативное обеспечение АБ аналитическими отчетами. Эти регистраторы событий могут быть реализованы как специальные программные модули в составе главных серверов областей или на базе отдельных программно- технических средств (firewall, маршрутизаторы и т.д.) и подотчетны только лишь АБ. Аналитические отчеты об угрозах в областях оперативно передаются регистраторами событий $e_f, f = \overline{1,F}$ к АБ по зашифрованным каналам. При попытке несанкционированной расшифровки этой информации аналитический отчет самоликвидируется. Собрав аналитические отчеты АБ анализирует ситуацию во всех областях и принимает оперативные меры по борьбе с имеющимся угрозами к ресурсам, отправляя к ним механизмы защиты по зашифрованным каналам. Следует особо подчеркнуть, что принятие решений в таких ситуациях является самым сложным процессом, т.к. АБ для устранения того или иного вида угроз, какие механизмы защиты должны быть задействованы. Обычно, в процессе разработки АБ, опираясь на практический опыт существующих компьютерных сетей, а также аналитических материалов международных организаций и ведущих компаний мира, специализирующихся в области информационной безопасности составляют перечень видов угроз и он может дополняться во время эксплуатации [1, 2, 3]. Следует отметить, что в зависимости от принятой политики безопасности угрозы в компьютерных сетях соответствующими администраторами безопасности могут восприниматься по разному. Так как, появление угрозы какого- либо типа в одной компьютерной сети, может вовсе не считаться угрозой в другой

компьютерной сети. Допустим, что рассматриваемый АБ, исходя из принятой политики безопасности, обеспечен информацией о существующем множестве $U = \left\{ u_j \middle| j = \overline{1,m} \right\}$ угроз, которые могут встречаться в областях компьютерной сети. Помимо этого, при функционировании АБ должны быть заданы (объявлены) стоимости защищаемых ресурсов. Предположим, что первоначальные стоимости ресурсов r_f равны d_{r_f}, $r_f = \overline{1,R_f}$, $f = \overline{1,F}$. Следовательно, первоначальная суммарная стоимость D всех ресурсов, принятых АБ для защиты равна:

$$D = \sum_{f=1}^{F} \sum_{r_f=1}^{R_f} d_{r_f}.$$

Главной задачей АБ является то, что в процессе функционирования компьютерной сети он должен осуществить такую стратегию борьбы с угрозами, которая приведет к самому минимальному ущербу от первоначальной суммарной стоимости D ресурсов за заданный срок эксплуатации. Таким образом, АБ вместе с регистраторами событий e_f, $f = \overline{1,F}$ составляют основу централизованной системы безопасности.

Теперь переходим к описанию детерминированной модели принятия решений АБ при борьбе с угрозами. Допустим, что регистраторы событий e_f, $f = \overline{1,F}$ через определенные моменты времени $t_1, t_2, \ldots, t_{k-1}, t_k, \ldots, t_n$ обеспечивают АБ аналитическими отчетами об угрозах, причем $\Delta t = t_k - t_{k-1} = const$ для всех $k = \overline{1,n}$. Здесь Δt выбирается с учетом времени t_A принятия решений АБ и максимального времени t_f передачи аналитических отчетов от регистраторов событий e_f к АБ по зашифрованным каналам

$$\Delta t > t_A + \max_f \left\{ t_f \right\}, \quad f = \overline{1,F}.$$

Известно, что ресурсы r_f в каждом моменте времени t_k будут подвергаться воздействиям угроз, в результате чего первоначальные и далее промежуточные стоимости ресурсов будут уменьшаться на определенную сумму, т.е.:

$$d_{r_f} \geq d_{r_f}(t_1) \geq \ldots \geq d_{r_f}(t_{k-1}) \geq d_{r_f}(t_k) \geq \ldots \geq d_{r_f}(t_n), \quad r_f = \overline{1,R_f}, \quad f = \overline{1,F}.$$

Следовательно,

$$D \geq D(t_1) \geq \ldots \geq D(t_{k-1}) \geq D(t_k) \geq \ldots \geq D(t_n).$$

Теперь введем параметр p_{jr_f}, характеризующий мощности угроз u_j по отношению к ресурсам r_f, который определяется непрерывно в отрезке [0, 1], т.е. $0 \leq p_{jr_f} \leq 1$. Если $p_{jr_f} = 1$, то угроза типа u_j при наступлении в момент t_k к ресурсу r_f наносит полный ущерб на сумму $d_{r_f}(t_k)$ и $p_{jr_f} = 0$, то ни какого ущерба не наносит. В общем виде, эти отношения опишем при помощи матрицы $P = \left\| p_{jr_f} \right\|$ мощностей угроз по отношению к ресурсам, где $j = \overline{1,m}$, $f = \overline{1,F}$, $r_f = \overline{1,R_f}$. Аналогично, введем параметр q_{ij}, характеризующий механизм защиты z_i по отношению к угрозе типа u_j, где $0 \leq q_{ij} \leq 1$. Здесь если $q_{ij} = 1$, то механизм защиты z_i полностью ликвидирует угрозы типа u_j, если $q_{ij} = 0$, то механизм z_i при борьбе с угрозой

типа u_j полностью бессилен, т.е. ни какую защиту не может осуществлять. Данные отношения опишем матрицей $Q=\|q_{ij}\|$, $i=\overline{1,l}$, $j=\overline{1,m}$. Отметим, что значения параметров p_{jr_f} и q_{ij} определяются на основании статистических и экспертных данных, представленных авторитетными организациями (COAST, NIST Computer Security Division 893, FIRST, ICSA и т.д.), занимающимися проблемами информационной безопасности [3, 4]. Наряду с этими параметрами, АБ выделяется определенная стоимость (бюджет на заданный срок) D_z для нормального функционирования при борьбе с угрозами в моментах времени $t_1 \div t_n$. Данная стоимость составляет определенную долю от первоначальной суммарной стоимости D, т.е. $D_z << D$. АБ в каждом моменте времени t_k из выделенной ему суммы D_z израсходует не более чем $D_z(t_k)$, другими словами бюджет распределяется среди моментов времени:

$$D_z = \sum_{z=1}^{m} D_z(t_k).$$

Известно, что АБ при задействовании механизмов защиты для борьбы с угрозами несет определенные затраты. Обозначим эти затраты при помощи матрицы $D'_z = \|d_{ijr_f}\|$, где d_{ijr_f} затраты АБ при задействовании механизма защиты z_i для борьбы с угрозой типа u_j, которая создает опасность к ресурсу r_f в области f. Здесь затраты d_{ijr_f} определяются с учетом месторасположения ресурсов r_f от АБ, вида и характеристик используемых защищенных каналов, по которым передаются механизмы защиты к областям для борьбы с возникшими угрозами, а также стоимости d_{r_f} ресурсов и соотношения значений параметров q_{ij} и p_{jr_f}. Отметим, что АБ при принятии решений в каждом моменте времени t_k для борьбы с угрозами извлекает из аналитических отчетов регистраторов событий e_f информацию о состоянии и количествах угроз к тому или иному ресурсу. С этой целью, информацию о состоянии угроз опишем при помощи бинарного параметра $x_{jr_f}(t_k)$, который если $x_{jr_f}(t_k)=1$, то в момент t_k в области f есть угроза типа u_j к ресурсу r_f, если $x_{jr_f}(t_k)=0$, то в противном случае. Соответственно, количество угроз типа u_j, появившихся в момент t_k в области f к ресурсу r_f обозначим через $k_{jr_f}(t_k)$. Анализ показывает, что уровень опасности к тому или иному защищаемому ресурсу в момент t_k зависит от значений параметров p_{jr_f}, q_{ij} и $k_{jr_f}(t_k)$, которые входят в формулу $\beta_{ijr_f}(t_k)$ следующим образом:

$$\beta_{ijr_f}(t_k) = k_{jr_f}(t_k)(1-q_{ij})p_{jr_f}.$$

Рассмотрим случай когда $\beta_{ijr_f}(t_k)>1$. Это говорит о том, что ущерб угрозой типа u_j с количеством $k_{jr_f}(t_k)$ к ресурсу r_f в момент t_k, когда АБ принимает решение задействовать механизм защиты z_i, равен $\beta_{ijr_f}(t_k)d_{r_f}(t_k)$, который в логическом смысле не реален. Потому, что максимальный ущерб в момент t_k к ресурсу r_f не может быть больше чем $d_{r_f}(t_k)$. Если $\beta_{ijr_f}(t_k)<1$, то будет нанесен ущерб к ресурсу

r_f частично, а при $\beta_{ijr_f}(t_k)=1$- полностью. В связи с этим, введем коэффициент опасности, определяемый по следующей формуле:

$$\alpha_{ijr_f}(t_k)=\begin{cases}1, & \text{если } \beta_{ijr_f}(t_k)\geq 1\\ \beta_{ijr_f}(t_k), & \text{если } \beta_{ijr_f}(t_k)<1\end{cases} \quad (1)$$

И так АБ располагая заданными матрицами P и Q, получая от регистраторов событий e_f, $f=\overline{1,F}$ в каждый момент времени t_k значения $k_{jr_f}(t_k)$ вычисляет эти коэффициенты для всех $i=\overline{1,I}$, $j=\overline{1,m}$, $r_f=\overline{1,R_f}$, $f=\overline{1,F}$. На основании этих данных АБ принимает решения о назначении механизмов защиты для борьбы с угрозами. В этой связи, введем нижеописанную псевдобулевую переменную, зависимую от момента времени t_k

$$y_{ijr_f}(t_k)=\begin{cases}1, & \textit{если АБ задействует механизм защиты } z_i \textit{ для борьбы с}\\ & \textit{угрозой типа } u_j, \textit{которая создает опасность к ресурсу } r_f\\ & \textit{в области } f \textit{ в момент } t_k;\\ 0, & \textit{в противном сл.}\end{cases}$$

Поскольку в каждом моменте времени от первоначальной стоимости d_{r_f} ресурса r_f отнимается определенный ущерб, для которого можем написать следующую формулу:

$$\delta_{ijr_f}(t_k)=x_{jr_f}(t_k)\alpha_{ijr_f}(t_k)y_{ijr_f}(t_k)\cdot\left[d_{r_f}-\sum_{s=0}^{k-1}\delta_{ijr_f}(t_s)\right],\quad k=\overline{1,n} \quad (2)$$

при начальном условии $\delta_{ijr_f}(t_0)=0$. Отметим, что в формуле (2)

$$d_{r_f}(t_k)=d_{r_f}-\sum_{s=0}^{k-1}\delta_{ijr_f}(t_s),$$

где $d_{r_f}(t_k)$ стоимость ресурса r_f в момент t_k. Тогда суммарный ущерб для момента времени t_k будет равен:

$$D_u(t_k)=\sum_{i=1}^{I}\sum_{j=1}^{m}\sum_{f=1}^{F}\sum_{r_f=1}^{R_f}\delta_{ijr_f}(t_k),\quad k=\overline{1,n}. \quad (3)$$

При этом реальные затраты АБ в моменте времени t_k будет определяться следующим образом:

$$D_z^*(t_k)=\sum_{i=1}^{I}\sum_{j=1}^{m}\sum_{f=1}^{F}\sum_{r_f=1}^{R_f}x_{jr_f}(t_k)y_{ijr_f}(t_k)d_{ijr_f},\quad k=\overline{1,n}. \quad (4)$$

Таким образом, с учетом вышеизложенного описания процесс функционирования АБ и формул (1)÷(4)можем привести детерминированную модель принятия решений при борьбе с угрозами:

$$D(t_k)=D(t_{k-1})-D_u(t_k)\to\max,\quad k=\overline{1,n} \quad (5)$$

при ограничениях:

$$D_z^*(t_k)\leq D_z(t_k)+\left[D_z(t_{k-1})-D_z^*(t_{k-1})\right],\quad k=\overline{1,n}, \quad (6)$$

$$\sum_{i=1}^{I}x_{jr_f}(t_k)y_{ijr_f}(t_k)=1,\quad j=\overline{1,m},\quad f=\overline{1,F},\quad r_f=\overline{1,R_f},\quad k=\overline{1,n}, \quad (7)$$

$$\sum_{j=1}^{m} x_{jr_f}(t_k) y_{ijr_f}(t_k) \le m, \quad i=\overline{1,l}, \quad f=\overline{1,F}, \quad r_f=\overline{1,R_f}, \quad k=\overline{1,n}, \tag{8}$$

$$\sum_{f=1}^{F} x_{jr_f}(t_k) y_{ijr_f}(t_k) \le F, \quad i=\overline{1,l}, \quad j=\overline{1,m}, \quad r_f=\overline{1,R_f}, \quad k=\overline{1,n}, \tag{9}$$

$$\sum_{r_f=1}^{R_f} x_{jr_f}(t_k) y_{ijr_f}(t_k) \le R_f, \quad i=\overline{1,l}, \quad j=\overline{1,m}, \quad f=\overline{1,F}, \quad k=\overline{1,n}. \tag{10}$$

В формулах (5) и (6) должны учитываться начальные условия $D(t_0)=D$, $D_z(t_0)=0$ и $D_z^*(t_0)=0$. Приведенная модель с рекуррентной структурой относиться к классу задач дискретного программирования с псевдобулевыми переменными [5]. По формуле (5) целевой функционал, характеризующий, что из стоимости $D(t_k)$ в каждом моменте времени t_k должен отниматься минимальный ущерб за счет оптимального назначения АБ механизмов защиты к угрозам. Формула (6) означает, что реальные затраты $D_z^*(t_k)$ АБ за момент времени t_k не должны быть больше, чем суммы выделенной (запланированной) стоимости $D_z(t_k)$ и остаточной стоимости $\left[D_z(t_k) - D_z^*(t_{k-1})\right]$ от предыдущего момента времени t_{k-1}. С другой стороны, это условие предусматривает, что сэкономленные средства в предыдущем моменте времени переходит к следующему моменту времени, в результате чего АБ приобретает больше возможностей для принятия более оптимальных решений при борьбе с угрозами. Как отмечалось выше, процесс принятия решений АБ осуществляется до запланированного момента времени t_n. При этом предусматривается, что максимальный суммарный ущерб к моменту времени t_n не будет больше, чем заданное значение ΔD, т.е.:

$$D - D(t_n) \le \Delta D.$$

Однако могут появиться такие ситуации когда АБ не достигая до момента времени t_n данное условие нарушается. При этом случае дальнейшее функционирование АБ считается не допустимым. В связи с этим, принимаются оперативные меры для выхода из данного положения: увеличивается бюджет АБ (D_z), включаются в состав множества Z более мощные механизмы защиты, за счет использования высокоскоростных каналов связи уменьшается интервал времени Δt приема аналитических отчетов от регистраторов событий e_f, с учетом накопленного опыта и новых рекомендаций международных организаций еще раз уточняются значения параметров p_{jr_f}, q_{ij} и т.д.

Таким образом, вышеприведенная детерминированная модель с рекурретной структурой реализуется как специальный программный модуль, который войдет в состав АБ компьютерной сети в качестве отдельного функционального блока принятия решений при борьбе с угрозами.

Литература

[1]. Сколот Н. *Безопасность информационных систем.* В журнале: Компьютер пресс, июнь 1998, сс.117-123.

[2]. Fisher L.F. *The threat to automated data systems.* Report «Security awareness» of

Department of defense security Institute, US; 1997.

[3]. Коржов В. *Защитники сетей.* В журнале: Сети, №4/97, сс. 116-122. http: // www.osp.ru/nets/1997/04/source/116.html.

[4]. Николаев А. *Технологии антивирусной защиты сети.* В журнале: Компьютер пресс, июнь 1998, сс.275-290.

[5]. Сергиенко И.В. *Математические модели и методы решения дискретной оптимизации.* 2-е изд. -Киев: Науково думка, 1998, 472с.