МОДЕЛЬ ОЦЕНКИ БЕЗОПАСНОСТИ СЛОЖНОЙ СЕТИ (ЧАСТЬ 2)

Калашников А.О.[1], Бугайский К.А.[2], Молотов А.А.[3]

Цель статьи: *разработка механизма оценивания действий агентов сложных информационных систем с точки зрения информационной безопасности.*

Метод исследования: *теоретико-игровой подход с использованием стохастического моделирования.*

Полученный результат: *определены типовые операции нарушителя и защитника. Разработана теоретико-игровая модель на основе игры с природой для определения результатов атаки на отдельный элемент сложной сети. На основе игры с нулевой суммой разработана модель противоборства агентов, базирующаяся на результатах игры с природой. Для игры с природой и игры с нулевой суммой определены стратегии действий агентов. Дано формальное описание модели и показано, что результат моделирования определяется шестью параметрами, не зависящими от конкретного вида графа сети.*

Научная новизна: *состоит в том, что рассмотрение противоборства агентов как двухуровневой составной игры позволяет моделировать поведение агентов в ходе противоборства. Это обеспечивается тем, что результаты розыгрыша игры нижнего уровня определяют состояние игры верхнего уровня, стратегии агентов на каждом из двух вложенных уровней рассматриваются независимо, а также на том, что моделирование стратегий агента-нарушителя проводится с учетом возможностей, предоставляемых всеми захваченными им узлами сложной сети.*

Ключевые слова: *модель информационной безопасности, оценка сложных систем, метод Монте-Карло, стратегия противоборства, игра с природой.*

DOI:10.21681/2311-3456-2022-5-47-60

Введение

В первой части статьи [1] было показано, что решение задач по защите информации может быть представлено как противоборство нарушителя и защитника в рамках теоретико-игровой модели. При этом сама информационная система (далее – ИС) представляется в форме «взвешенного» графа, а действия нарушителя и защитника – агентов, – как выполнение определенных действий над элементами ИС – вершинами или узлами графа (точнее – их весами). Противоборство рассматривается как стремление достичь главной цели того или иного агента: попытка нарушить параметры «конфиденциальности – целостности – доступности» (далее – параметры КЦД) узлов ИС со стороны нарушителя и противодействие этим попыткам со стороны защитника (иными словами – сохранение текущих параметров КЦД). В модели принято, что необходимым и достаточным условием для достижения главной цели является получение агентом пользовательских или системных права доступа на узле, иными словами – стать «владельцем» узла или части процессов и/или документов этого узла. Сам процесс противоборства агентов представлен в модели как перемещение агентов по узлам графа, связанное с изменением их «весов» и подчиненное достижению их главной цели. При этом каждому узлу графа для каждого агента может быть поставлена в соответствие определенная локальная цель. Достижение локальной цели («захват» узла) считается реализованным только в случае успешного выполнения всех операций соответствующего набора. Успешность выполнения операций и достижения локальных целей отображаются в модели изменением статуса узла и расчетом затрат

1 К л шников Андрей Олегович, доктор технических н ук, гл вный н учный сотрудник л бор тории «Сложных сетей» ФГБУН Институт проблем упр вления им. В.А. Тр пезников РАН, г. Москв , Россия. E mail: aokalash@ipu.ru

2 Буг йский Конст нтин Алексеевич, мл дший н учный сотрудник л бор тории «Сложных сетей» ФГБУН Институт проблем упр вления им. В.А. Тр пезников РАН, г. Москв , Россия. E-mail: kabuga@ipu.ru

3 Молотов Алекс ндр Ан тольевич, инженер-прогр ммист НВО-89 Институт проблем упр вления им. В.А. Тр пезников РАН, г. Москв , Россия. E-mail: alpha.sphere@ya.ru

и приобретений ресурса агента. Которые, в свою очередь, рассматриваются как результат игры агента с природой в силу функционирования агента в условиях неопределенности.

Описание операций

В модели принято, что действия агента состоят из последовательности операций. Опишем (на основании [2-15]) базовый перечень операций агента, который позволит конкретизировать действия агента и более предметно рассматривать реализацию локальных целей как игру с природой.

Базовый перечень операции для описания действий нарушителя

ОН1. Операция получения информации о текущем состоянии узла и доступных для него связях. Например, список исполняемых процессов, доступных программ и документов, настройки сетевых интерфейсов и статистика по обмену данными с другими узлами. Данная операция должна предшествовать практически всем действиям нарушителя.

ОН2. Операция получения информации о смежных узлах. Например, пассивное или активное сканирование смежных узлов с целью определения доступных для атаки портов, протоколов, процессов, типов программного обеспечения (далее – ПО) и так далее. Данная операция используется при реализации действий ДН1, ДН2, ДН4 (см. первую часть статьи [1]).

Действия ДН3, ДН5 (см. первую часть статьи [1]) предполагают проведение активной фазы атаки на узел. С учетом сделанных выше предположениях будем считать, что все многообразие средств и методов атак на узел ИС сводится к изменению прав доступа нарушителя на данном узле. Введем операцию:

ОН3. Операция получение прав пользователя на узле. При этом подразумевается получение как прав пользователя, так и системных прав (суперпользователя).

Действия ДН3, ДН5 также предполагают внесение изменений в перечни ПО, процессов и пользователей с соответствующим приданием этому необходимых прав для работы. Соответственно, введем операции:

ОН4. Операция записи на узле.

ОН5. Операция установки прав на узле.

Относительно операции ОН4 следует отметить, что в широком смысле операция записи предполагает практически любые действия по нарушению параметров КЦД на узле. Поскольку сюда можно отнести и изменения конфигурации и манипуляции с доступными процессами и документами. Таким образом, можно говорить о сочетании последовательностей операций ОН4 и ОН5 для различных действий.

Например, действие ДН5 может быть описано как последовательность операций:

ОН1, ОН2, ОН3 (пользователь), ОН4, ОН5 (внедрение деструктивного ПО (далее – ДПО)), ОН3 (суперпользователь), ОН5, ОН4 (манипуляции с узлом).

Базовый перечень операции для описания действий защитника.

О31. Операция получения информации о текущих настройках (состоянии) узла и доступных для него связях. Например, список исполняемых процессов, доступных программ и документов, настройки сетевых интерфейсов и статистика по обмену данными с другими узлами. Данная операция должна предшествовать практически всем действиям защитника.

О32. Операция получения информации о доступных узлах. Что можно трактовать как получение информации от всех узлов, определенных ранее в качестве точек мониторинга или получивших усиление защиты (см. раздел Описание противоборства).

В деятельности защитника можно отметить определенную двойственность. С одной стороны, защитник по определению должен иметь достаточные права на узле для выполнения своих функций. Но, с другой стороны, это не отменяет необходимости для защитника выполнять операции аутентификации и авторизации, а также выполнять определенные действия от имени других зарегистрированных пользователей на узле. В случае необходимости оперативного реагирования на действия нарушителя защитник может выполнять действия связанные с изменениями конфигурации узла, а также различные манипуляции с доступными процессами и документами включая изменения прав доступа. Соответственно, целесообразно ввести следующие операции:

О33. Операция получения (реализации) прав пользователя на узле. При этом подразумевается получение как прав пользователя, так и системных прав (суперпользователя).

О34. Операция записи на узле.

О35. Операция установки прав на узле.

Следует уточнить, что приведенный выше перечень операций для нарушителя и защитника не является закрытым и может дополняться, и расширяться. Важно также отметить, что предлагаемая в модели конструкция «действие состоит из операций» дает возможность гибко учитывать архитектурные и функциональные особенности как различных узлов ИС, так и ИС в целом.

Описание игры с природой

Использование в модели игры с природой основано на том, что в каждый конкретный момент времени агент находится на определенном узле и должен решить следующие задачи:

— выбор атакуемого на данном шаге узла;
— выбор локальной цели для атакуемого узла;
— выполнение необходимого набора операций по достижению локальной цели.

Для осуществления выбора необходимо иметь варианты и критерии выбора. В качестве вариантов для выбора узла для атаки в модели используются смежные узлы, которые образуют строки платежной матрицы. Для осуществления выбора локальной цели используются определенные в первой части действия в зависимости от типа агента – нарушитель или защитник. Указанные действия образуют столбцы платежной матрицы игры с природой. То есть, для платежной матрицы такой игры локальной стратегией агента является выбор одного из инцидентных, для текущего узла, ребер графа, а в качестве вариантов реализации – те или иные действия агента. На основании механизмов, предложенных в первой части статьи [1], производится розыгрыш всех возможных сочетаний узел-действие (локальная цель) доступных агенту в данный момент времени. То есть имеем игру $\Gamma^z(V^\delta, \Psi^z)$, где:

$V^\sigma \in V$ – множество смежных узлов из всех вершин *V* графа ИС;

Ψ^z – множество действий агента типа $z = \{h, d\}$, где *h* и *d* нарушитель и защитник соответственно;

$\Psi_i^z = \{o_1, \dots, o_j\}$, $o_j \in O^z$, где O^z – множество операций доступных агенту для выполнения действия Ψ_i^z.

Входные параметры игры определены в первой части статьи [1] и задаются перед началом игры:

w_v, $v \in V^\sigma$ – ценность узла;

ρ_o , $o \in O^z$ – сложность операции;

θ – квалификация агента;

μ_v, $v \in V^\sigma$ – состояние узла.

Выходные (рассчитываемые) параметры игры также определены в первой части статьи [1]:

C^z – множество затрат агента на выполнение операций O^z по достижению локальных целей Ψ^z на доступных узлах ;

B^z – множество выигрышей агента за счет повышения информированности или снятия неопределенности в результате выполнение операций O^z по достижению локальных целей Ψ^z на доступных узлах V^σ;

T^z – множество ходов в игре O^z (количество повторов операций до достижения успеха каждого действия Ψ^z на каждом узле V^σ).

Тогда ячейка платежной матрицы M^z игры Γ^z имеет вид:

$$m_{v,\psi} = \{c_v^\psi, b_v^\psi, t_v^\psi\} \quad (1),$$

где: $c_v^\psi \in C^z$, $b_v^\psi \in B^z$, $t_v^\psi \in T^z$.

При этом величины c_v^ψ, b_v^ψ, t_v^ψ считаются нарастающим итогом $x := x + y$ по всем операциям для каждого смежного узла.

Полученное в результате розыгрыша игры Γ^z заполнение ячеек платежной матрицы M^z является основой для определения перемещения агента по графу за счет осуществления выбора узла и выбора конкретного действия в отношении его со стороны агента. В рамках модели результатом игры с природой является выбор конкретной ячейки матрицы M^z. Состав ячейки платежной матрицы (1) позволяет использовать для выбора затраты, выигрыш и число ходов агента. Вопросы выбора агентом узла и действия с одновременным использованием всех величин из состава ячейки платежной матрицы являются предметом дальнейших исследований. Как будет показано далее, использование той или иной конкретной величины из c_v^ψ, b_v^ψ, t_v^ψ для осуществления выбора ячейки $m_{v,\psi}$ определяется в общем виде стратегией агента. Таким образом, для получения результата игры с природой необходимо выполнить две операции выбора на основе одной из указанных величин: выбрать строку – захватываемый узел и выбрать столбец – реализованную локальную цель.

Выбор узла будем производить с точки зрения минимизации ошибки выбора узла. Для этого воспользуемся критерием Сэвиджа [5]. Из исходной матрицы M^z. построим матрицу M' с помощью критерия выбора k так, чтобы ячейки M' содержали только одну из величин c_v^ψ , b_v^ψ , t_v^ψ , то есть:

$$m_{v,\psi} km_{ij} \text{ и } m_{ij} = \{c, b, t\} \quad (2).$$

Столбцы матрицы j по-прежнему соответствуют действиям агента, а строки i – смежным узлам. Для каждого столбца найдем максимальную величину $y_j = \max\left(m_{ij}\right)$ и разницу $x_{ij} = y_j - m_{ij}$. В результате получим матрицу риска X. Для каждой строки этой матрицы определим наибольшую величину $x_i^+ = \max\left(x_{ij}\right)$. Тогда выбор строки – то есть выбор узла $v_k \in V^\sigma$ для выполнения действий – будет определяться:

— для c_v^ψ – затрат агента – $v_k : c_k = \max\left(x_i^+\right)$ (3);
— для b_v^ψ – выигрыш агента – $v_k : b_k = \min\left(x_i^+\right)$ (4);
— для t_v^ψ – число выполненных операций агента –

$v_k : t_k = \max\left(x_i^+\right)$ (5).

Таким образом, агент выбирает узел как строку в матрице платежей игры с природой, отвечающую минимизации риска выбора. Выбор действия (столбца матрицы) определяется как ценностью выбранного узла, так и предпочтениями агента в данный момент времени. Обозначим предпочтения агента как $\varphi \in [0,1]$ при условии $\sum_{i=1}^{|\psi|}\varphi_i = 1$. В рамках модели положим, что предпочтения агента определяются применяемой им тактикой достижения глобальной цели. В общем виде это можно рассматривать как поведенческую характеристику агента. В силу чего целесообразно определять значения φ на основании розыгрыша для каждого действия агента.

Как показано в первой части статьи [1], каждому действию агента поставлена в соответствие кажущаяся ценность узла $\omega = \pi w_v$, как доля от «истинной» ценности w_v, где $\pi \in [0,1]$ – задаваемый коэффициент соответствия. В рамках модели полагаем, что по результатам игры с природой агент снижает информационную неопределенность относительно выбранного узла. Что, в свою очередь, вызывает изменение кажущейся ценности узла. На основании энтропийного подхода результат игры с природой позволяет рассматривать коэффициент π как функцию от усилий на выполнение действий, приводящих к снижению информационной неопределенности агента. Как показано в первой части статьи [1], минимально необходимые усилия определяют пороговое значение успешности выполнения операций, что позволяет определить коэффициент соответствия для отдельного действия как:

$$\pi_\psi = \sum_{i=1}^{\tau}\delta_i / \tau \quad (6),$$

где:

τ – число операций в составе действия;

δ_i – пороговое значение вероятности успешного выполнения операции.

Тогда кажущая ценность узла в результате успешного выполнения данного действия в рамках игры с природой может быть определена как:

$$\omega_v^\psi = \pi_\psi w_v \quad (7).$$

Примем кажущую ценность узла для данного действия ω_v^ψ в качестве порогового значения относительно которого будем рассматривать полученные в результате розыгрыша данного действия значения затрат c_ψ и выигрыша b_ψ.

Сформируем оценочные значения затрат для каждого действия $i \in \Psi$ на основании разницы между пороговым и текущим значениями $\epsilon_i = \omega_i - c_i$:

$$x_i = \begin{cases}\epsilon_i - \epsilon_i\varphi_i, c_i < \omega_i \\ \epsilon_i + \epsilon_i\varphi_i, c_i > \omega_i\end{cases}$$

Тогда выбор действия по значениям затрат определяется правилом:

$$\psi = \min\left(x_i\right) \quad (8).$$

Аналогично поступим и для выигрыша, определив разницу как $\epsilon_i = b_i - \omega_i$:

$$x_i = \begin{cases}\epsilon_i - \epsilon_i\varphi_i, b_i < \omega_i \\ \epsilon_i + \epsilon_i\varphi_i, b_i > \omega_i\end{cases}$$

Тогда выбор действия по значениям затрат определяется правилом:

$$\psi = \max\left(x_i\right) \quad (9).$$

Для выбора действия на основе числа ходов t_ψ в качестве порога выберем необходимое число операций в отдельном действии τ_ψ. Сформируем оценочные значения на основании разницы между пороговым и текущим значениями $\epsilon_i = \tau_i - t_i$, $i \in \Psi$:

$$x_i = \begin{cases}\epsilon_i - \epsilon_i\varphi_i, t_i < \tau_i \\ \epsilon_i + \epsilon_i\varphi_i, t_i > \tau_i\end{cases}$$

И выбор действия по числу ходов определим по правилу:

$$\psi = \min\left(x_i\right) \quad (10).$$

Таким образом, на основании розыгрыша игры с природой осуществляется выбор конкретного узла и определенного действия с этим узлом. Что дает основание рассматривать результат игры с природой Γ^z как функцию выбора определенной ячейки из платежной матрицы игры M^z. Если рассматривать понятие «агент» обобщенно, то следует говорить о множестве агентов, каждый из которых относится к подмножеству нарушителей или защитников: $A = H \bigcup D$, где A – множество агентов, H – подмножество нарушителей, D – подмножество защитников. Соответственно, уточним величину z: $z = \begin{cases}h, a \in H \\ d, a \in D\end{cases}$. Обозначим результат игры с природой агента: $L^z\left(\Gamma_a^z\right) = F\left(M^z\right)$, где: $z = \{h,d\}$, $a \in A$. На основании выражений (3-5,8-10) можно положить, что функция выбора представляет собой отношение $\prec$, формируемое на основе задаваемых

предпочтений агента φ и критерия Сэвиджа применительно к одному из выбранных параметров (2). Тогда стратегия агента определяется для всех смежных узлов как $S_a = \{C^z, B^z, T^z, k_a, \varphi_a, \prec, V^\sigma\}$, где: $z = \{h, d\}$, $a \in A$. Применение стратегии дает результат достижения локальной цели (захват узла), выражаемый в затратах, выигрыше и потраченном числе ходов.

В первой части статьи [1] было показано, что затраты и выигрыш агента могут быть представлены в безразмерных единицах ресурса. А также, что выигрыш агента, как снятие неопределенности является аддитивной функцией. Данное обстоятельство позволяет говорить о возможности расчета баланса ресурса агента как итогового показателя его деятельности. Если $X(t)$ – значение показателя по выполнению хода *t*, то тогда баланс агента в результате игры с природой может быть представлен как:

$$D(t) = D(t-1) - C(t) + B(t) \qquad (11).$$

Поскольку выражение (11) представляет собой рекуррентную функцию, логично положить, что любой агент для участия в игре должен иметь некоторую стартовую величину ресурса $D_a(t_0)$, где $a \in A$.

Розыгрыш игры с природой можно рассматривать как отдельный шаг в противоборстве нарушителя и защитника. Тогда получаемые результаты $L^h\left(\Gamma_a^h\right)$ и $L^d\left(\Gamma_a^d\right)$ представляют собой исходные данные для описания противоборства нарушителя и защитника

Описание противоборства нарушителя и защитника

В данном варианте модели противоборство защитника и нарушителя мы будем рассматривать с позиций нарушителя. То есть прежде всего моделируя возможные действия нарушителя по реализации атаки и уже на этой основе – меры противодействия защитника. Следует особо подчеркнуть, что действия защитника будут рассматриваться с точки зрения уменьшения возможностей нарушителя по развитию атаки.

Противоборство с точки зрения нарушителя

На графе ИС выделяем конкретный узел, который является стартовой позицией нарушителя. При этом данный узел не может быть изменен или сделан недоступным нарушителю (отключен, занят защитником) на все время работы модели с установленными параметрами. В случае моделирования действий внешнего нарушителя данный стартовый узел рассматривается как внешний по отношению к графу ИС. В этом случае перед стартом работы модели он должен быть соединен ребрами с определенными узлами графа ИС. Порядок формирования таких ребер определяется характером подключения ИС к внешним каналам связи. В случае моделирования внутреннего нарушителя стартовый узел выбирается (директивно или случайным образом) из числа узлов графа ИС. При этом никаких изменений в составе инцидентных ребер этого узла не производится.

Глобальная цель нарушителя с точки зрения описания его перемещений по графу может задаваться, например, следующим образом:

Вариант 1. Цель – задается конкретный конечный узел на графе ИС, выбираемый директивно или случайным образом. В этом случае на графе ИС определяется подграф игры, который содержит все возможные пути из стартового в конечный узел. В дальнейшем предполагается, что все перемещения нарушителя ограничиваются узлами данного подграфа. Данный вариант можно рассматривать как модель целевой атаки на ИС, прежде всего с целью нарушения конфиденциальности.

Вариант 2. Цель – задается конкретная глубина проникновения в ИС в виде максимальной длины пути на графе, которую он должен достичь. В этом случае на графе ИС определяется подграф игры, который содержит все возможные пути из стартового в конечные узлы. В дальнейшем предполагается, что все перемещения нарушителя ограничиваются узлами данного подграфа.

Вариант 3. Цель – задается доля узлов графа ИС, которые нарушитель должен захватить.

Варианты 2 и 3 могут рассматриваться как модели атак на закрепление на определенном уровне в ИС с целью последующих операций по нарушению параметров КЦД. В качестве примера можно привести получение доступа к технологическому сегменту АСУ ТП, работу вымогательских группировок, создание ботнетов и др. Перемещение нарушителя по графу (подграфу) игры осуществляется последовательно от узла к узлу и только по инцидентным ребрам. Основанием для перемещения к следующему узлу является захват текущего узла, что можно рассматривать как достижение нарушителем локальной цели для атакуемого в данный момент времени узла.

Дадим следующие определения

Ход игры (шаг) – достижение локальной цели агентом.

Ход агента – выполнение агентом определенной операции из числа необходимых для достижения локальной цели.

Управляющий узел – узел ИС, обеспечивающий функционирование инфраструктуры ИС. Например, такие как контроллеры домена, что дает возможность получить не только данные авторизации подчиненных узлов, но также логическую и сетевую и структуру данного домена ИС

Так как речь идет о моделировании действий нарушителя в сложной сети, то целесообразно положить, что на каждом шаге нарушитель имеет возможность реализовывать локальную цель для одного из нескольких смежных (текущему) узлов. Для моделирования перемещений нарушителя введем следующие критерии, определяющие его поведение на основе гипотезы о его рациональности.

Критерий 1. Минимизация собственных усилий на достижение локальной цели, то есть минимальное расходование имеющихся в распоряжении нарушителя ресурсов.

Критерий 2. Максимизация скрытности действий, то есть достижение локальной цели за минимальное число ходов (повторов операций до достижения успеха). Поскольку принято, что время в модели рассматривается как последовательность шагов и операций.

Критерий 3. Максимальное снятие неопределенности действий агента по достижению глобальной цели.

Учет для определения поведения нарушителя критерия 3 позволяет положить, что нарушитель будет стремиться захватывать управляющие узлы, обеспечивающие функционирование инфраструктуры ИС. Для упрощения правил модели мы будем считать, что захват управляющих узлов на графе является обязательным только в случае их смежности текущему узлу нахождения нарушителя.

Критерий 4. Повышение неопределенности действий защитника, то есть захват узлов на графе с целью маскирования цели перемещений по графу.

Учет для определения поведения нарушителя критерия 4 позволяет положить, что подобные маскирующие действия могут совершаться ограничено, поскольку противоречат критериям 1 и 2. Для упрощения правил модели положим, что захват узла с целью маскирования действий возможен в случае, если этот узел не имеет инцидентных ребер к узлам на требуемом пути к глобальной цели. Кроме того, положим, что захват узла вне пути к цели возможен в случае, когда затраты на его захват меньше ожидаемого прироста ресурса в случае захвата.

Критерий 5. Нанесение максимального ущерба защитнику в ходе достижения локальной цели.

Данный критерий следует рассматривать как стремление нарушителя получить максимальные полномочия на захваченном узле – суперпользователя или системные полномочия. Максимизация ущерба в этом случае следует из возможности нарушителя нарушить параметры КЦД любым доступным способом. Например:

- отключить действия средств защиты и мониторинга;
- осуществить изменение режимов работы узла в своих интересах;
- внести изменения в состав действующих процессов и применяемого ПО;
- внести изменения в распределение прав доступа пользователей.

В основе моделирования перемещений нарушителя лежит алгоритм стягивания ребра между текущим и захватываемым узлом. Это не только позволяет избежать циклов в деятельности нарушителя (повторный захват узлов), но и соответствует реальному положению дел, когда для продолжения атаки нарушитель может использовать любой захваченный им ранее узел. Обозначим:

- V^H – множество узлов, захваченных нарушителем,
- $v^0 \in V^H$ – текущий узел нахождения нарушителя,
- $V^+ \notin V$ – множество «новых» узлов смежных текущему.

Тогда можно выделить следующие типы ребер $e(v_1, v_2),\ e \in E$ для текущего узла:

- $e^0(v_i, v^0),\ v_i \in V^+ \wedge v_i \notin V^{\mathrm{H}}$ – инцидентные текущему узлу,
- $e^H(v_i, v^0),\ v_i \in V^{\mathrm{H}} \wedge v_i \notin V^+$ – между текущим и захваченными ранее узлами,
- $e^-(v_i, v_j),\ v_i \in V^{\mathrm{H}} \wedge v_j \in V^+ \wedge v_i \neq \neq v_j \wedge (v_i, v_j) \neq v^0$ – между смежными текущему и захваченными ранее узлами,
- $e^+(v_i, v_j)$ $v_i \in V^{\mathrm{H}} \wedge v_j \notin (V^+ \vee V^{\mathrm{H}}) \wedge v_i \neq v_j \wedge (v_i, v_j) \neq \neq v^0$ – между захваченными ранее узлами и смежных им.

Соответственно, с учетом стягивания ребер между захваченными узлами, полный список V^σ смежных узлов для текущего формируется по следующему правилу: $v_i \in V^\sigma$ если $\exists\left(e^0 \vee e^- \vee e^+\right)$.

Для упрощения модели в части сокращения вычислений положим, что очередной розыгрыш игры с природой проводится только для узлов $v_i \in V^+$, но

при этом нарушитель обладает памятью и матрица платежей игры с природой должна строиться с учетом связей типа e^+ и e^-, то есть с учетом результатов имевших в этих случаях розыгрышей. Это позволит при выборе ячейки платежной матрицы в качестве результата текущего розыгрыша игры с природой учесть все доступные нарушителю возможности по выбору узла атаки и действия на нем.

Но для связей типа e^- и e^0 возникает проблема выбора только одного из результатов текущего и предыдущего розыгрышей. Это означает, что среди захваченных нарушителем узлов существует как минимум два, которые могут использоваться для захвата следующего узла. Пусть такие узлы образуют множество V^g. Для решения этой проблемы сделаем следующее допущение: характеристики узла, связанные со сложностью операций ρ_o и состоянием узла μ_v могут различаться для разных инцидентных ребер узла. Это дает возможность построить матрицу M'', ячейки которой содержат одну из величин c_v^ψ, b_v^ψ, t_v^ψ, то есть $m_{ij} = \{c, b, t\}$. Данная матрица строится относительно атакуемого узла и служит выбору одного из узлов $v_j \in V^g$, который будет использоваться агентом для атаки. Столбцы матрицы по-прежнему соответствуют действиям агента. Выбор строки матрицы осуществляется на основании модифицированного критерия Гурвица. Полагаем, что предпочтения агента φ в данном случае определяются параметрами атакуемого узла и едины для всех узлов $v_j \in V^g$ из состава матрицы M''. Находим столбцы k и l для которых предпочтения агента φ имеют соответственно максимальное φ^+ и минимальное φ^- значения. Для каждой из строк матрицы рассчитываем коэффициент $g_i = \varphi^+ m_{ik} + \bar{\varphi} m_{il}$. Выбор строки матрицы M'' осуществляем по следующим правилам: $\max(g_i)$ для выигрыша агента и $\min(g_i)$ для затрат и числа ходов. Выбранный таким образом узел и соответствующая строка ячеек, содержащих c_v^ψ, b_v^ψ, t_v^ψ включается в состав платежной матрицы M^z для последующего определения результатов розыгрыша игры с природой при условии наличия памяти у нарушителя.

В заключении отметим, что любые действия нарушителя по реализации локальной цели (захвата узла) начинаются в условиях отсутствия у него прав доступа на узле. За исключением случаев доступа с захваченного ранее управляющего узла.

Противоборство с точки зрения защитника

На графе ИС выделяем конкретный узел, который является стартовой позицией защитника. Стартовый или начальный узел выбирается (директивно или случайным образом) из числа узлов графа ИС. При этом никаких изменений в составе инцидентных ребер этого узла не производится. При этом данный узел не может быть изменен или сделан недоступным защитнику (отключен, удален) на все время работы модели с установленными параметрами.

Моделирование поведения защитника основано на его способности перемещаться в течение одного хода игры на любой узел графа. Это положение базируется на том, что современные ИС имеют развитые средства защиты и мониторинга состояния узлов, обеспечивающие централизованные сбор и обработку информации. Это означает что:

- защитник владеет всей информацией о структуре графа ИС: обо всех узлах и связях;
- защитник обладает необходимыми правами доступа и полномочиями для выполнения действий по защите информации на узлах;
- защитник имеет возможность определять текущее состояние любого узла.

То есть все узлы графа при моделировании противоборства со стороны защитника рассматриваются как смежные его стартовому узлу. Так как речь идет о моделировании действий защитника в современной ИС, то целесообразно положить, что на каждом шаге защитник имеет возможность реализовывать локальную цель для одного из нескольких смежных узлов. Таким образом, шаг игры для защитника состоит в перемещении со стартового узла на один из узлов графа («виртуальный»), выполнение действий на одном или нескольких смежных с виртуальным узлах и возврат на стартовый узел. С соответствующим расчетом его затрат и выигрыша, а также числа ходов.

Вместе с тем моделирование противоборства предполагает, что для определения состояния узла или изменения этого состояния, защитник должен произвести захват данного узла. То есть реализовать те или иные действия (локальную цель), связанные с получением (активацией) имеющихся у него права доступа на узле. Как следует из описания действий и операций защитника, его локальные цели, определяемые противодействием развитию атаки нарушителя, предполагают приданию узлам на графе свойств точек мониторинга, дающим информацию о действиях нарушителя или усиление защитных свойств узлов на предполагаемой трассе движения нарушителя по графу. Свойства мониторинга и защищенности определены в первой части статьи как состояние узла $\mu = \{\mu^H, \mu^D\}$.

Состояние узла в процессе выполнения соответствующих действий защитником определяются по ре-

зультатам розыгрыша случайной величины. Обозначим μ^0 как текущее значение состояния узла. Тогда новое значение определяется как $\mu^+ \in [\mu^0, 1]$. Целесообразно положить, что значение $\mu > 0.5$ следует рассматривать как назначение узла точкой мониторинга независимо от функциональности ($\{\mu^H, \mu^D\}$). Такой подход позволяет допустить захват нарушителем стартового узла защитника. В этом случае стартовым узлом назначается одна из существующих точек мониторинга. В рамках рассматриваемой модели противоборства будем полагать, что защитник не обладает памятью, то есть он может многократно захватывать один и тот же узел и последовательно менять его состояние. При этом все операции для таких действий выполняются независимо от предыдущих результатов. Для упрощения модели положим, что защитник получает информацию от точки мониторинга автоматически при выполнении определенных условий. К таким условиям следует прежде всего отнести попытки захвата узла со стороны нарушителя, в том числе и попытки активного сканирования узла.

Глобальная цель защитника с точки зрения описания его перемещений по графу может задаваться, например, следующим образом:

Вариант 1. Цель – задается конкретный конечный узел на графе ИС. В большинстве случаев данный конечный узел должен представлять собой точку мониторинга, от которой поступил сигнал о действиях нарушителя. Но возможны (особенно на начальном этапе игры) и варианты задания конечного узла директивно или случайным образом. Такой вариант можно рассматривать как модель целевого противодействия атаке на конкретный узел ИС (например, точку доступа к определенной подсети). В дальнейшем предполагается, что перемещения защитника на смежные узлы ограничиваются инцидентными ребрами данного узла.

Вариант 2. Цель – задается конкретный набор конечных узлов. Этот набор задается директивным или случайным образом. В этом случае на графе ИС определяется подграф игры, который содержит стартовый узел, все конечные узлы и смежные с ними. В дальнейшем предполагается, что все перемещения защитника ограничиваются данным подграфом. Перемещение защитника по конечным узлам подграфа осуществляется последовательно или случайно.

Варианты 1 и 2 предполагают, что после захвата узла смежного с конечным узлом, защитник имеет возможность:

- двигаться далее только по инцидентным ребрам (аналогично нарушителю); основанием для перемещения к следующему узлу является захват текущего узла;
- вернуться на стартовый узел для последующих действий.

Вариант 3. Цель – на графе ИС задаются начальный и конечный узлы. В этом случае на графе ИС определяется подграф игры, который содержит все возможные пути из начального в конечный узел. В дальнейшем предполагается, что все перемещения защитника ограничиваются узлами данного подграфа. Данный вариант можно рассматривать как модель контроля возможной трассы целевой атаки на ИС. По достижению конечного узла защитник должен вернуться на стартовый узел.

Для моделирования перемещений защитника введем следующие критерии, определяющие его поведение на основе гипотезы о его рациональности.

Критерий 1. Минимизация собственных усилий на достижение локальной цели, то есть минимальное расходование имеющихся в распоряжении защитника ресурсов.

Критерий 2. Максимизация эффективности действий, то есть достижение локальной цели за минимальное число ходов (повторов операций до достижения успеха). Поскольку принято, что время в модели рассматривается как последовательность шагов и операций.

Критерий 3. Максимальное снятие неопределенности действий агента по достижению глобальной цели, то есть захват узла, имеющего максимальное число инцидентных ребер.

Учет для определения поведения защитника критерия 3 основан на том, что в этом случае обеспечивается возможность проверки состояния большего числа узлов без необходимости возврата на стартовый узел.

Критерий 4. Минимизация ущерба для защитника от действий нарушителя. С другой стороны, данный критерий может формулироваться для нарушителя как максимизация ущерба, наносимого защитнику. Отметим, что обе трактовки предполагают выполнение агентом тех или иных действий на путях, ведущих к наиболее ценным узлам ИС.

Уточним, что все указанные в данном подразделе конечные узлы для защитника следует рассматривать и как точки мониторинга, доступные ему на постоянной основе.

Приведенные варианты действий нарушителя и защитника не могут рассматриваться как «чистые» стратегии агентов, поскольку, во-первых, они не

являются исчерпывающими, а во-вторых, они могут применяться агентами в различных сочетаниях в процессе достижения глобальной цели. С другой стороны, все варианты действий агентов обладают общими критериями как для нарушителя, так и для защитника. Приведенные описания игры с природой и вариантов противоборства нарушителя и защитника, позволяют сделать вывод о том, что в основе деятельности агента лежит оперирование критериями на основе затрат, выигрыша и скрытности (оперативности) действий, то есть числа ходов. Исходя из выражений (2-5) можно определить следующие критерии работы агента для достижения глобальной цели:

— Критерий скрытности или оперативности действий: $K_T^z = \min_{v_i \in V^\sigma} T_a^z(v_i)$ (12);

— Критерий затрат: $K_C^z = \min_{v_i \in V^\sigma} C_a^z(v_i)\}$ (13);

— Критерий выигрыша: $K_B^z = \max_{v_i \in V^\sigma} B_a^z(v_i)$ (14).

Здесь, в выражениях для критериев, приведенных выше: $a \in A$, $z = \{h,d\}$ и $v_i \in V^\sigma$ это смежные с текущим узлы графа.

Указанные критерии (12-14) используются агентами в каждой игре с природой для каждого смежного узла с целью определения дальнейшего продвижения по графу. При этом распределение критериев (12-14) по узлам $\mathcal{F}: K \to V$ является прямым отображением поведения нарушителя и защитника. Поскольку именно от глобальной цели и текущей информированности агент принимает решение о характере последующих действиях: обеспечить максимальную скрытность, снизить затраты (усилия) или максимально снизить уровень неопределенности. Таким образом, можно говорить о наличии стратегии противоборства нарушителя и защитника, направленной на достижение глобальной цели агента: $\mathbb{S} = \{K_T^z, K_C^z, K_B^z, \mathcal{F}, V\}, z = \{h,d\}$ и базирующейся на функции $\mathcal{F}$ распределения критериев по узлам.

В модели принято, что результаты реализации стратегии агента отображаются в статусе узлов, в отношении которых агентом совершались те или иные действия. Статус прежде всего должен отражать способность агента манипулировать параметрами КЦД. Данные манипуляции определяют ущерб ИС от действий нарушителя. Для упрощения модели будем рассматривать нарушения параметров КЦД со стороны нарушителя, поскольку в модели не предусмотрено восстановление параметров КЦД со стороны защитника. В общем виде эти отношения можно представить как:

Успех операции => Успех действия => Изменения статуса узла => Ущерб.

Сделаем следующие допущения.

1) В модели принято три типа для определения прав пользователей на узлах: системный, авторизованный и неавторизованный (гостевой).

2) Каждый узел имеет тип в соответствии с его конфигурацией и/или функциональным предназначением. Представляется целесообразным ввести следующие типы по функциональному предназначению: управляющий, родительский, подчиненный, автономный.

3) Тип узла описывается весовыми коэффициентами, отражающими важность каждого из параметров КЦД для данного узла: $\xi^К$ – для конфиденциальности, $\xi^Д$ – для целостности и $\xi^Д$ – для доступности, при условии $\xi^* \in [0,1]$.

4) Для каждого типа прав пользователя введем весовой коэффициент, отражающий возможности манипуляции параметрами КЦД: $\eta^К$ – для конфиденциальности, $\eta^Ц$ – для целостности и $\eta^Д$ – для доступности; при условии $\eta^* \in [0,1]$.

Указанные допущения позволяют ввести коэффициент ущерба для узла:

$$\omega_v^R = \eta^К \xi^К + \eta^Ц \xi^Ц + \eta^Д \xi^Д \quad (15).$$

Если положить, что системному пользователю доступно все возможности по нарушению КЦД ($\eta^К = \eta^Ц = \eta^Д = 1$), а неавторизованный пользователь может только нарушить доступность ($\eta^К = \eta^Ц = 0$ и $\eta^Д = 1$), то коэффициент ущерба для узла может меняться в диапазоне от 0 до 3. Отметим еще раз, что ущерб появляется в результате успешных действий нарушителя, дающих ему возможности (права доступа) по манипулированию параметрами КЦД. Тогда с учетом (7) и (15) можем определить, что суммарный ущерб для защитника со стороны нарушителя представляет собой выражение:

$$W = \sum_{i=1}^{|V^H|} \omega_{v_i}^R \omega_{v_i}^\psi, \quad (16),$$

где $v_i \in V^H$ и V^H – число захваченных нарушителем узлов.

Отметим, что результаты игры с природой, определяющие достижение агентом локальной цели, могут в силу сложности сети давать несколько равнозначных значений по выбору захватываемого узла и соответствующего действия. Приведенные рассуждения позволяют ввести критерий ущерба, обеспечивающий выбор такого узла и получение таких прав доступа нарушителем, что дает максимальный ущерб:

$K_W^h = \max\limits_{v_i \in V^\sigma}\left(\omega_{v_i}^R \omega_{v_i}^\psi\right)$. Соответственно, для защитника критерий должен обеспечивать минимизацию ущерба: $K_W^d = \min\limits_{v_i \in V^\sigma}\left(\omega_{v_i}^R \omega_{v_i}^\psi\right)$. При этом $v_i \in V^\sigma$ это смежные с текущим узлы графа. Таким образом, стратегия противоборства нарушителя и защитника, направленная на достижение глобальной цели агента, может быть записана как: $\mathbb{S} = \left\{K_W^z, K_T^z, K_C^z, K_B^z, \mathcal{F}, V\right\}$, $z = \{h, d\}$.

Как было предложено ранее полагаем, что время в игре едино для всех агентов и представляет собой последовательность определенных дискретных шагов. Из чего следует, что число ходов игры Γ^0 должно быть одинаково для защитника и нарушителя. Обозначим t_i^a, $a \in A$ как i-й ход агента a по выполнению операции и n^a как число ходов этого агента. Тогда:

$$T^d = \sum_{j=1}^{|D|}\sum_{i=1}^{n^{d_j}} t_i^{d_j}$$

$$T^h = \sum_{j=1}^{|H|}\sum_{i=1}^{n^{h_j}} t_i^{h_j}$$

$$T^d = T^h = T \qquad (17)$$

Здесь: T – число шагов игры Γ^0 и перед ее началом должно задаваться предельное значение T^0. Соответственно, каждый ход агента приводит к уменьшению числа шагов: $T = T - 1$.

Завершая описание противоборства нарушителя и защитника, отметим особую роль управляющих узлов, которая выражается в том, что агент получает определенные преимущества, облегчающие достижение локальных целей на узлах, так или иначе подчиненных управляющему. Для упрощения модели будем предполагать, что при выполнении захвата подчиненного узла стратегия $\mathbb{S}$ вырождается до вида: $\mathbb{S} = \{\mathcal{F}, V\}$, где функция распределения $\mathcal{F}$ означает случайный выбор одного из подчиненных и смежных узлов. Кроме того, стратегия выбора результата игры с природой приобретает вид $S_a = \left\{\varphi_a, V^\sigma\right\}$, то есть определяется исключительно предпочтениями агента. Соответственно, расчет выигрыша, затрат и числа ходов при достижении локальной цели производится при условии низкой сложности операций и состояния узла: $\mu = \rho = 0.1$, а также высокой квалификации агента и вероятности успешного выполнения операции: $\theta = p = 0{,}9$.

Общее описание модели

Модель представляет противоборство защитника и нарушителя как перемещение агентов по узлам ИС в рамках достижения ими глобальной и локальных целей.

ИС представляет собой граф $G(E, V)$ со множествами связей E и вершин V, которые являются отображением узлов ИС и их взаимодействия на уровне сетевой доступности.

Узлы ИС составляют множество вершин графа $v \in V$ и каждый узел описывается кортежем $v = \langle uidV, typeV, catV, w, parID, cntID, \Psi, R, DomV\rangle$, где:

$uidV$ – уникальный идентификатор узла (вершины);

$typeV = \{type1, type2, \ \}$ – тип узла, подразумевающий отнесение узла к определенному типу в соответствии с его конфигурацией и/или функциональному предназначению;

$catV = \{parV, cntV, basV\}$ – категория узла, где: $cntV$ – управляющий узел, $parV$ – узел-контейнер (например, сервер ВМ), $basV$ – базовый (типовой) узел;

w – ценность узла;

$parID$ – идентификатор узла-контейнера для данного узла;

$cntID$ – идентификатор управляющего узла для данного узла;

$\Psi = \left\{\psi^h, \psi^d\right\}$ – список доступных действий, определяемый раздельно для нарушителя и защитника;

R – статус узла, определяемый по результатам выполнения действий;

$DomV = \{uidV1, uidV2, \ldots\} \exists uidV \ catV = parV \vee cntV$ – дополнительная характеристика для управляющих узлов и узлов-контейнеров, представляющая собой список подчинённых или вложенных узлов.

Все элементы кортежа – кроме R – задаются при формировании графа ИС и остаются неизменными в процессе работы модели. Задание и изменение статуса узла описано ниже.

Связи графа $e \in E$ описываются кортежем: $e = \langle uidE, uidV, \mu, \rho\rangle$, где:

$uidE$ – уникальный идентификатор связи;

$uidV$ – уникальный идентификатор инцидентного узла;

$\mu = \left\{\mu^h, \mu^d\right\}$, $\mu \in [0,1]$ – состояние узла, определяемое раздельно для нарушителя и защитника;

$\rho = \left\{\rho^h, \rho^d\right\}$, $\rho \in [0,1]$ – сложность операции узла, определяемая раздельно для нарушителя и защитника;

Элементы кортежа $uidE$, $uidV$ задаются при формировании графа ИС и остаются неизменными в процессе работы модели. Элементы кортежа μ, ρ за-

даются при формировании графа ИС и изменяются в процессе работы модели.

Агенты, определяемые в модели, образуют множество и каждый из них относится к одному из подмножеств – нарушители или защитники: $A = H \bigcup D$, $H \bigcap D = \varnothing$. Агент $a \in A$ представлен кортежем:

$a = \langle uidA, typeA, catA, \theta, \Psi, D, DomA \rangle$, где:

$uidA$ – уникальный идентификатор агента;

$typeA = \{type1, type2, \ \}$ – тип агента на основе его функционала (например, администратор ВМ, администратор ИБ);

$catA = \{h, d\}$ – *категория агента: нарушитель или защитник;*

$\theta \in [0,1]$ – квалификация агента;

Ψ – список доступных действий, определяемый типом и категорией агента;

D – размер доступного агенту ресурса, определяемый как баланс между затратами и выигрышем при выполнении доступных действий.

$DomA = \{uidV1, uidV2, \ \}$ – область действия агента, прежде всего для защитников разных типов, представляющая перечень доступных узлов с определенными правами доступа.

Все элементы кортежа – кроме D и $DomA$ – определяются при построении модели и не изменяются в процессе ее работы. Баланс доступного ресурса агента D задается в начале игры как начальный ресурс и пересчитывается в процессе работы модели. Область действия агента определяется в начале игры и изменяется в процессе работы модели. Изменения области действия агента отражаются в статусе узлов R по результатам выполняемых агентами действий.

Статус узла описывается кортежем:

$R = \langle uidA, Status \rangle$, где:

$uidA$ – идентификатор агента;

$Status7 \ \{Na, Auth, Sys, Scan, None, Pot\}$ – статус узла, где:

Na – узел доступный агенту с правами гостя (без авторизации) то есть, прежде всего с точки зрения сетевой доступности;

$Auth$ – узел доступный агенту с правами пользователя;

Sys – узел доступный агенту с системными правами;

$Scan$ – узел, подвергшийся воздействию агента без изменения прав доступа (например, полное сканирование нарушителем или контроль текущего состояния защитником);

$None$ – узел недоступный агенту;

Pot – общедоступный или незащищенный узел (например, киберфизическое устройство, о котором известно, что оно скомпрометировано или созданная защитником приманка).

Перечень действий, которые могут совершать нарушитель и защитник, задаются при построении модели раздельно для нарушителя и защитника и не изменяются в процессе ее работы $\Psi = \Psi^h \bigcup \Psi^d$, $\Psi^h \bigcap \Psi^d = \varnothing$. Каждое действие описывается кортежем:

$\Psi = \langle OP, \pi, \varphi, C, B, T \rangle$, где:

$OP = \{o_1, \ , o_i, \ , o_\tau\}, o_i \in O^z$, $z = \{h, d\}$ – количество (τ) операций доступных агенту для выполнения действия Ψ_j^z. Перечень операций для каждого действия также задается при построении модели и не изменяется в процессе ее работы;

π – коэффициент соответствия, представляющий действию кажущуюся стоимость узла, задается при построении модели и не изменяется в процессе ее работы;

φ – предпочтения агента, могут изменяться на каждом шаге игры;

C – затраты агента на выполнение действия, рассчитывается в процессе работы модели;

B – выигрыш агента при успешном выполнении действия, рассчитывается в процессе работы модели. Действие считается успешным, если успешно выполнены все операции из его состава, а операция успешна – если вероятность успешного выполнения превышает порог δ (определен в первой части статьи [1]).

T, $T \geq \tau$ – число ходов агента (выполненных операций), изменяется в процессе работы модели.

Каждое действие совершается тем или иным агентом в отдельный момент времени (ход модели) применительно к конкретному узлу. Для упрощения модели примем, что совместные действия различных агентов в отношении отдельного узла в каждый момент времени не допустимы. Вопросы совместной работы агентов, прежде всего в части кооперации защитников, являются предметом дальнейшего исследования.

Модель рассматривает противоборство защитника и нарушителя с теоретико-игровой точки зрения как игру Γ^0 с нулевой суммой. Шаги игры Γ^0 представляют собой поочередное выполнение агентами действий по получению полномочий на узле графа осуществляемое в условиях неопределенности. Условия неопределенности позволяют рассматривать действия агентов как игру с природой. Обозначим Γ^h как ход нарушителя, а Γ^d как ход защитника. Тогда противоборство нарушителя и защитника может быть представлено как:

$$\Gamma^0 = \{\Gamma_1^h, \Gamma_1^d, \ldots, \Gamma_n^h, \Gamma_n^d\} \quad (18),$$

где n – число шагов (ходов игры Γ^0).

Выражения (11, 17, 18) позволяют считать, что время (как последовательность событий) является общим как для игры Γ^0, так и для игры с природой Γ^z, $z=\{h,d\}$. Игра с природой описана ранее и ее результатом являются рассчитанные значения C, B, T – затрат, выигрыша и числа ходов агента при выполнении конкретного действия. В соответствии с (11) на основании C и B производится расчет баланса агента D. Как было показано ранее (варианты 1-3 глобальной цели нарушителя и защитника), цели агентов не могут быть представлены в качестве конкретных результатов игры Γ^0, приводящих к ее останову. Прежде всего в силу информационной неопределенности защитника относительно целей и методов их достижения со стороны нарушителя. А для нарушителя – в силу информационной неопределенности структуры ИС, средств и методов защиты. Соответственно, возникает проблема останова работы модели. Представляется целесообразным положить, что останов работы модели происходит по достижению заданного значения ущерба W^0 ($W \geq W^0$), а также при исчерпании заданного лимита ходов $\left(T^0 \to 0\right)$ или при отсутствии у любого агента ресурса для выполнения очередного действия ($D \to 0$). Из (18) следует, что содержание ячеек платежной матрицы M^0 игры Γ^0 определяется результатами игр Γ^z. С точки зрения анализа безопасности сложной сети платежная матрица M^0 должна обеспечивать общую оценку результатов деятельности агентов в ходе противоборства нарушителя и защитника. Соответственно (в отличие от классического варианта для игры с нулевой суммой) целесообразно в качестве строк платежной матрицы использовать перечень агентов, а в качестве столбцов – их стратегии, представляющие собой распределение критериев выбора по узлам сети. Ячейки m^0 платежной матрицы M^0 в этом случае должны содержать результаты работы модели для каждого агента: W – нанесенный ущерб (16), D – текущий баланс (11) и затраченное число ходов T (17), а также перечень захваченных агентом узлов V^a *в ходе работы модели*:

$$m_{as}^0 = \left\{D^a, T^a, W, \mathrm{V}^a\right\} \quad (19),$$

где: $s \in \mathbb{S}$, $a \in A$.

Напомним, что стратегия достижения глобальной цели агента в ходе противоборства представляет собой функцию $\mathcal{F}$ распределения критериев K_W^z, K_T^z, K_C^z, K_B^z по узлам графа. Данные критерии совместно с предпочтениями агента φ формируют стратегию игры с природой, обеспечивающей достижение локальной цели. В свою очередь, достижение локальной цели зависит от вероятности успешной реализации операций p (см. первую часть статьи [1]). Модель предполагает, что все эти три величины – $\mathcal{F}$, φ и p – определяются в результате розыгрыша случайной величины методом Монте-Карло. Кроме того, изменение состояния узла μ и сложности операции ρ в ходе выполнения отдельных действий защитником также проводится как розыгрыш случайной величины. Наконец, расчеты модели используют такую характеристику как квалификация агента θ (см. первую часть статьи [1]).

Таким образом, результаты работы модели (18) непосредственно зависят от шести переменных: θ, μ, ρ, $\mathcal{F}$, φ и p. Изменение которых позволяет проводить анализ безопасности сложной сети с разных точек зрения даже при условии неизменности графа узлов (структуры) ИС.

Заключение

Разработанная модель анализа безопасности сложной сети позволяет осуществлять стохастическое моделирование действий нарушителя и защитника на основе ограниченного числа параметров. Результаты работы модели позволяют проводить не только оценку безопасности структуры ИС, представленной в виде графа, но и поведенческие аспекты деятельности нарушителя в рамках противоборства с защитником. Разработанные механизмы расчетов основных показателей деятельности нарушителя и защитника (затраты, выигрыш, ущерб, оперативность и скрытность операций) позволяют развивать модель на уровне разработки правил без внесения изменений в эти механизмы. Модель предоставляет основу для изучения вопросов связанных с кооперацией агентов при анализе безопасности сложной сети.

Литература

1. Калашников А.О. Модель оценки безопасности сложной сети (Часть 1) / А.О. Калашников, К.А. Бугайский // Вопросы кибербезопасности. – 2022. – № 4 – С. 26-38.
2. DOI:10.21681/2311-3456-2022-4-26-38
3. Дойникова Е. В. Оценка защищенности компьютерных сетей на основе метрик CVSS / Е.В. Дойникова, А.А. Чечулин, И.В. Котенко // Информационно-управляющие системы. – 2017. – № 6(91). – С. 76-87. – DOI 10.15217/issn1684-8853.2017.6.76

4. Пучков В. В. Анализ защищенности киберфизических систем с использованием графов атак / В.В. Пучков, И. В. Котенко // Информационная безопасность регионов России (ИБРР-2021) : Материалы конференции, Санкт-Петербург, 27–29 октября 2021 года. – Санкт-Петербург: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления». 2021. – С. 98-100.
5. Дойникова Е.В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью / Е. В. Дойникова, И. В. Котенко. – Москва : Российская академия наук. 2021. – 184 с.
6. Зеличенок И. Ю. Анализ методов выявления многошаговых атак / И. Ю. Зеличенок, И. В. Котенко // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей в 4х томах, Санкт-Петербург, 24–25 февраля 2021 года / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. 2021. – С. 400-405.
7. Левшун Д. С. Проблемные вопросы информационной безопасности киберфизических систем / Д.С. Левшун, Д. А. Гайфулина, А. А. Чечулин, И. В. Котенко // Информатика и автоматизация. – 2020. – Т. 19. – № 5. – С. 1050-1088.
8. Середкин С.П. Моделирование угроз безопасности информации на основе банка угроз Федеральной службы по техническому и экспортному контролю России / С.П. Середкин // Информационные технологии и математическое моделирование в управлении сложными системами. 2022. – № 1(13). – С. 43-54.
9. Сердечный А. Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой APT29 в распределенных компьютерных системах / А. Л. Сердечный, П. С. Краюшкин, М. А. Тарелкин, Ю. К. Язов // Информация и безопасность. 2021. – Т. 24. – № 1. – С. 83-92.
10. Сердечный А. Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой APT3 в распределенных компьютерных системах / А. Л. Сердечный, А. В. Айдаркин, М. А. Тарелкин, А. Е. Дешина // Информация и безопасность. 2021. – Т. 24. – № 1. – С. 35-46.
11. Егошин Н. С. Модель типовых угроз безопасности информации, основанная на модели информационных потоков / Н. С. Егошин // Доклады Томского государственного университета систем управления и радиоэлектроники. 2021. – Т. 24. – № 3. – С. 21-25.
12. Будников С. А. Моделирование APT-атак, эксплуатирующих уязвимость Zerologon / С.А. Будников, Е. Е. Бутрик, С. В. Соловьев // Вопросы кибербезопасности. – 2021. – № 6(46). – С. 47-61. DOI:10.21681/2311-3456-2021-6-47-61
13. Кондаков С. Е. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий / С. Е. Кондаков, И. С. Рудь // Вопросы кибербезопасности. 2021. – № 5(45). – С. 12-20. DOI:10.21681/2311-3456-2021-5-12-20
14. Овчаров В. А. Подход к профилированию поведения нарушителя на основе моделирования тактик, техник и процедур проведения компьютерных атак / В. А. Овчаров, И. А. Соловьев, Н. А. Трофимова, А. Ф. Шинкаренко // Труды Военно-космической академии имени А.Ф. Можайского. 2021. – № 679. – С. 137-148.
15. Ерышов В. Г. Моделирование процесса защиты объектов критической информационной структуры промышленных предприятий от компьютерных атак / В. Г. Ерышов, Р. Д. Куликов // Морской вестник. 2021. – № 1(77). – С. 91-96.
16. Хованских С. А. Методика защиты распределенных вычислений в многоагентной системе / С.А. Хованских, В. А. Литвиненко, В. С. Хованская // Известия ЮФУ. Технические науки. 2019. – № 4(206). – С. 68-80.
17. Колентеев Н.Я. Принятие решений в условиях природной неопределенности / Н.Я. Колентеев, А.С. Кобелева // Специальная техника и технологии транспорта. 2020. – № 8(46). – С. 286-293.

A MODEL FOR ASSESSING THE SECURITY OF A COMPLEX NETWORK (PART 2)

Kalashnikov A.O.[4], Bugajskij K.A.[5], Molotov A.A.[6]

Purpose of the article: *development of a mechanism for evaluating the actions of agents of complex information systems from the point of view of information security.*

Research method: *game-theoretic models using stochastic modeling methods.*

The result: *typical operations of the violator and defender are defined. A game-theoretic model based on a game with nature has been developed to determine the results of an attack on a separate element of a complex network. Based on the zero-sum game, a model of agent confrontation based on the results of the game with nature has been developed. For the game with nature and the zero-sum game, the strategies of agents' actions are defined. A*

4 Andrey O. Kalashnikov, Dr.Sc., Chief Scientist of the Laboratory «Complex networks» Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: aokalash@ipu.ru

5 Konstantin A. Bugajskij, Junior Researcher of the Laboratory «Complex networks» Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E mail: kabuga@ipu.ru

6 Aleksandr A. Molotov, software engineer Research and Implementation Department №89 Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E mail: alpha.sphere@ya.ru

formal description of the model is given, and it is shown that the simulation result is determined by six parameters that do not depend on a particular type of network graph.

Keywords: *information security model, assessment of complex systems, Monte Carlo method, strategy of confrontation, playing with nature.*

References

1. Kalashnikov A.O. Model' ocenki bezopasnosti slozhnoj seti (Chast' 1) / A.O. Kalashnikov, K.A. Bugajskij // Voprosy kiberbezopasnosti. – 2022. – № 4 – S. 26-38. DOI:10.21681/2311-3456-2022-4-26-38
2. Dojnikova E. V. Ocenka zashhishhennosti komp'juternyh setej na osnove metrik CVSS / E.V. Dojnikova, A.A. Chechulin, I.V. Kotenko // Informacionno-upravljajushhie sistemy. – 2017. – № 6(91). – S. 76-87. – DOI 10.15217/issn1684-8853.2017.6.76
3. Puchkov V. V. Analiz zashhishhennosti kiberfizicheskih sistem s ispol'zovaniem grafov atak / V.V. Puchkov, I. V. Kotenko // Informacionnaja bezopasnost' regionov Rossii (IBRR-2021) : Materialy konferencii, Sankt-Peterburg, 27–29 oktjabrja 2021 goda. – Sankt-Peterburg: Regional'naja obshhestvennaja organizacija "Sankt-Peterburgskoe Obshhestvo informatiki, vychislitel'noj tehniki, sistem svjazi i upravlenija". 2021. – S. 98-100.
4. Dojnikova E.V. Ocenivanie zashhishhennosti i vybor kontrmer dlja upravlenija kiberbezopasnost'ju / E. V. Dojnikova, I. V. Kotenko. – Moskva : Rossijskaja akademija nauk. 2021. – 184 s.
5. Zelichenok I. Ju. Analiz metodov vyjavlenija mnogoshagovyh atak / I. Ju. Zelichenok, I. V. Kotenko // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii: sbornik nauchnyh statej v 4h tomah, Sankt-Peterburg, 24–25 fevralja 2021 goda / Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M.A. Bonch-Bruevicha. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M.A. Bonch-Bruevicha. 2021. – S. 400-405.
6. Levshun D. S. Problemnye voprosy informacionnoj bezopasnosti kiberfizicheskih sistem / D.S. Levshun, D. A. Gajfulina, A. A. Chechulin, I. V. Kotenko // Informatika i avtomatizacija. – 2020. – T. 19. – № 5. – S. 1050-1088.
7. Seredkin S.P. Modelirovanie ugroz bezopasnosti informacii na osnove banka ugroz Federal'noj sluzhby po tehnicheskomu i jeksportnomu kontrolju Rossii / S.P. Seredkin // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami. 2022. – № 1(13). – S. 43-54.
8. Serdechnyj A. L. Modelirovanie, analiz i protivodejstvie scenarijam komp'juternyh atak, realizuemyh gruppirovkoj APT29 v raspredelennyh komp'juternyh sistemah / A.L. Serdechnyj, P.S. Krajushkin, M.A. Tarelkin, Ju. K. Jazov // Informacija i bezopasnost›. 2021. – T. 24. – № 1. – S. 83-92.
9. Serdechnyj A. L. Modelirovanie, analiz i protivodejstvie scenarijam komp›juternyh atak, realizuemyh gruppirovkoj APT3 v raspredelennyh komp›juternyh sistemah / A. L. Serdechnyj, A. V. Ajdarkin, M.A. Tarelkin, A. E. Deshina // Informacija i bezopasnost›. 2021. – T. 24. – № 1. – S. 35-46.
10. Egoshin N. S. Model› tipovyh ugroz bezopasnosti informacii, osnovannaja na modeli informacionnyh potokov / N.S. Egoshin // Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki. 2021. – T. 24. – № 3. – S. 21-25.
11. Budnikov S.A. Modelirovanie APT-atak, ekspluatirujushhih ujazvimost› Zerologon / S.A. Budnikov, E. E. Butrik, S. V. Solov›ev // Voprosy kiberbezopasnosti. – 2021. – № 6(46). – S. 47-61. DOI:10.21681/2311-3456-2021-6-47-61
12. Kondakov S.E. Model› processa provedenija komp›juternyh atak s ispol›zovaniem special›nyh informacionnyh vozdejstvij / S.E. Kondakov, I.S. Rud› // Voprosy kiberbezopasnosti. 2021. – № 5(45). – S. 12-20. DOI:10.21681/2311-3456-2021-5-12-20
13. Ovcharov V.A. Podhod k profilirovaniju povedenija narushitelja na osnove modelirovanija taktik, tehnik i procedur provedenija komp›juternyh atak / V.A. Ovcharov, I.A. Solov›ev, N.A. Trofimova, A.F. Shinkarenko // Trudy Voenno-kosmicheskoj akademii imeni A.F. Mozhajskogo. 2021. – № 679. – S. 137-148.
14. Eryshov V. G. Modelirovanie processa zashhity ob#ektov kriticheskoj informacionnoj struktury promyshlennyh predprijatij ot komp›juternyh atak / V. G. Eryshov, R. D. Kulikov // Morskoj vestnik. 2021. – № 1(77). – S. 91-96.
15. Hovanskov S. A. Metodika zashhity raspredelennyh vychislenij v mnogoagentnoj sisteme / S.A. Hovanskov, V. A. Litvinenko, V. S. Hovanskova // Izvestija JuFU. Tehnicheskie nauki. 2019. – № 4(206). – S. 68-80.
16. Kolenteev N.Ja. Prinjatie reshenij v uslovijah prirodnoj neopredelennosti / N.Ja. Kolenteev, A.S. Kobeleva // Special›naja tehnika i tehnologii transporta. 2020. – № 8(46). – S. 286-293.