УДК 004.942

МОДЕЛИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ НЕССИМЕТРИЧНОГО КОНФЛИКТНОГО ВЗАИМОДЕЙСТВИЯ СИСТЕМ И ИХ ПРИМЕНЕНИЕ В ЗАДАЧАХ ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

А. А. Сирота, Н. И. Гончаров

Воронежский государственный университет

Поступила в редакцию 11.09.2018 г.

Аннотация. Рассматриваются математическая и компьютерная модели информационных процессов несимметричного конфликтного взаимодействия систем, характерного для задач исследования безопасности использования «облачных» технологий. В основе предложенных моделей лежит использование формализма гибридных автоматов. Получены аналитические соотношения для оценки нижней границы вероятности выигрыша одной из сторон в конфликте, позволяющие абстрагироваться от конкретного вида плотностей распределений для времени пребывания сторон в своих возможных состояниях. Рассмотрен пример применения моделей несимметричных конфликтных взаимодействий для исследования безопасности использования «облачных» технологий.
Ключевые слова: моделирование конфликта, карты состояний, гибридные автоматы, информационная безопасность, облачные системы, безопасность облачных технологий.
Annotation. The mathematical and computer models of information processes of asymmetric conflict interaction of systems typical for the problems of security research of the use of "cloud" technologies are considered. The proposed models are based on the use of hybrid automata formalism. Analytical relations are obtained to estimate the lower limit of the probability of winning one of the parties to the conflict, allowing to abstract from a particular type of density distributions for the time of stay of the parties in their possible States. An example of application of models of asymmetric conflict interactions for the study of security of the use of "cloud" technologies is considered.
Keywords: conflict modeling, state maps, hybrid automata, information security, cloud systems, security of cloud technologies.

ВВЕДЕНИЕ

Нарушение безопасности информации (БИ), циркулирующей в информационных системах, происходит в результате преднамеренных и непреднамеренных конфликтных взаимодействий систем с объектами внешней среды (нарушители, недобросовестные или неквалифицированные пользователи). Исследование закономерностей конфликта в задачах безопасности информационных систем (ИС), а также безопасности используемых в них информационных технологий позволяет формировать эффективные меры защиты и направления совершенствования таких систем и технологий.

В настоящее время, широкое распространение находят системы хранения, обработки и передачи данных, основанные на технологии «облачных» вычислений. Вместе с тем, в открытых источниках регулярно появляется информация о новых найденных уязвимостях в уже функционирующих «облачных» системах. Разработка гарантированно безопасных систем этого типа невозможна в силу самой идеи, положенной в основу технологии. Особое значение в такой ситуации приобретает фактор времени, определяющий возможности нарушения информационной безопасности при несвоевременном закры-

тии обнаруживаемых уязвимостей. Поэтому исследование закономерностей конфликтных взаимодействий информационных процессов и систем, построенных с использованием «облачных» технологий, является актуальной задачей.

Основные идеи современной теории конфликта [1–11] состоят в построении концептуальной модели, связывающей действующие объекты и факторы и направленной на установление закономерностей рационального поведения сторон в условиях конфликта. Для этого при моделировании всегда в той или иной форме реализуется представление конфликта в виде графа, описывающего набор возможных состояний систем и допустимые переходы между ними. В известных работах рассматриваются различные подходы к математическому моделированию конфликта систем: на основе аппарата сетей Петри [6], теории игр [7], теории активных систем [8], вероятностных сетей [9], теории динамических систем [10] и др.

Плодотворным подходом для построения математической и компьютерной модели конфликта является использование аппарата полумарковских случайных процессов (ПСП) [2–5, 11, 12, 13]. Тем не менее, при построении моделей на основе ПСП действует принципиальное ограничение: необходимо в явном виде задавать плотности распределения вероятностей для времени нахождения систем в своих состояниях. Часто эти плотности являются неизвестными, что приводит к необходимости проведения анализа для нескольких вариантов распределений, которые также до конца не обоснованы с физической точки зрения [12]. К числу недостатков подхода также следует отнести необходимость больших временных и трудовых затрат на аналитическое описание различных вариаций конфликта.

Естественным выходом в этой ситуации представляется использование средств компьютерного имитационного моделирования (ИМ), основанных на использовании объектных представлений, обеспечивающих описание конфликта в его естественном виде и возможность простой модификации моделей. Такие возможности, на наш взгляд, предоставляет формализм гибридных автоматов (ГА) и его многочисленные реализации в современных средствах ИМ. Их главной особенностью является представление каждого объекта – участника конфликта в виде диаграммы (карты) состояний, отражающих поведение этого объекта. Для описания процессов здесь не обязательно вводить свойство полумарковости или, даже, использовать статистическое представление. Ранее в работах авторов [14, 15] с использованием формализма ГА рассматривались модели симметричных конфликтных взаимодействий систем и коалиций систем, для которых характерно наличие эквивалентных целей и схожей структуры для участвующих в конфликте сторон.

Целью данной работы является обоснование типовых математической и компьютерной моделей несимметричного конфликтного взаимодействия систем, характерного для задач исследования безопасности использования информационных технологий на примере «облачных» технологий. В рамках предложенных моделей решается задача получения соотношений для оценки нижней границы вероятности выигрыша сторон в конфликте.

МЕТОДЫ И МАТЕРИАЛЫ

Математические и компьютерные имитационные модели разработаны с использованием формализма гибридных автоматов. Для реализации компьютерной имитационной модели с использованием формализма гибридных автоматов применялась среда Matlab+Simulink+Stateflow. Соотношения для приближённой оценки вероятности и нижней границы вероятности выигрыша сторон в конфликте получены на основе фундаментальных неравенств теории вероятностей. Проверка возможности использования полученных аналитических соотношений проводилась методом статистического имитационного моделирования. Основные свойства гибридных автоматов и их применение в задачах моделирования симметричных конфликтных взаимодействий систем рассматривались в предыдущих работах авторов [14, 15].

1. ТИПОВАЯ МОДЕЛЬ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ НЕСИММЕТРИЧНОГО КОНФЛИКТНОГО ВЗАИМОДЕЙСТВИЯ

При использовании гибридных автоматов (ГА) для моделирования и исследования конфликта систем всегда важно провести типизацию основных схем конфликтных взаимодействий [14, 15]. Рассмотрим описание типового несимметричного конфликта двух систем с разными целевыми функциями и структурой, который, на наш взгляд, характерен для задач исследования безопасности использования информационных систем, построенных с использованием «облачных» технологий.

Пусть в конфликте одной из сторон (сторона А) выступает облачная информационная система (ИС). Положительным результатом работы ИС, который можно рассматривать как выигрыш в конфликте, является обеспечение безопасности циркулирующей в ней информации в течение заданного промежутка времени $0 \le t \le T$. При этом ИС все время находится в группе состояний, характерных для ее эксплуатации и функционирования в штатных режимах, обеспечивающих целостность, конфиденциальность и доступность циркулирующей в ней информации. Отрицательным результатом функционирования «облачной» ИС (проигрышем в конфликте) является нарушение безопасности циркулирующей в ней информации, сопровождающееся переходом в соответствующее критическое состояние.

Второй стороной конфликта (сторона В) является другая система (система – нарушитель), которая преднамеренно или непреднамеренно может нарушить безопасность циркулирующей информации в А, что означает перевод «облачной» ИС в критическое состояние в пределах заданного интервала времени. Достижение данного результата определяет выигрыш системы – нарушителя (СН). Проигрыш В здесь возникает в случае не достижения результата за отведенный промежуток времени $0 \le t \le T$. Здесь и далее системы А и В, обозначения которых набраны прямым шрифтом, соответствуют гибридным автоматам A, B, для которых далее используются обозначения курсивом.

На основе математической схемы гибридного автомата (ГА) для моделирования и исследования несимметричного конфликтного взаимодействия с антагонистическими интересами рассмотрим следующую типизированную (обобщенную) модель, представленную на рис. 1. При ее описании будем использовать ранее введенные в [14, 15] понятия формализма гибридных автоматов.

В представленной на рис. 1 модели параллельно действует два ГА: автомат A и автомат B. Для этих автоматов множество дискретных переменных $S^D = \{s_a, s_b\}$, описывающих основные состояния, представлено двумя переменными, каждая из которых принимает значения $s_a \in Q_A = \{L_A, D_A\}$, $s_b \in Q_B = \{L_B, D_B\}$. Состояние L_A здесь обозначает функционирование A до момента использования противником имеющейся уязвимости, что ведет к «проигрышу» A и переходу в критическое состояние D_A («смерть» A). Состояние L_B здесь обозначает функционирование B с целью нарушения работы A, которое продолжается до истечения отведенного для этого времени, что ведет к «проигрышу» B («смерть» B) и соответствующему переходу в состояние D_B. Переход в D_A и D_B происходит скачкообразно под влиянием событий $attack\_B$ и $t \ge T$, определяющих, соответственно, проигрыш для A и B. Соответственно, формально $Q = Q_A \times Q_B$. Удобно также ввести множества $L = \{L_A, L_B\}$, $D = \{D_A, D_B\}$. Состояния из совокупности D в данной модели являются поглощающими. Стрелки с черным кружком обозначают начальные состояния (здесь состояния L_A, L_B).

Для детального и адекватного описания поведения сторон в условиях конфликта предлагается ввести внутреннее описание состояний из множества $L = \{L_A, L_B\}$ в виде вложенных гибридных автоматов, которые будем называть гибридными автоматами активных элементов (ГА АЭ). Главным преимуществом подобной схемы является возможность агрегированного описания возможности перехода в состояния D. В противном случае следо-

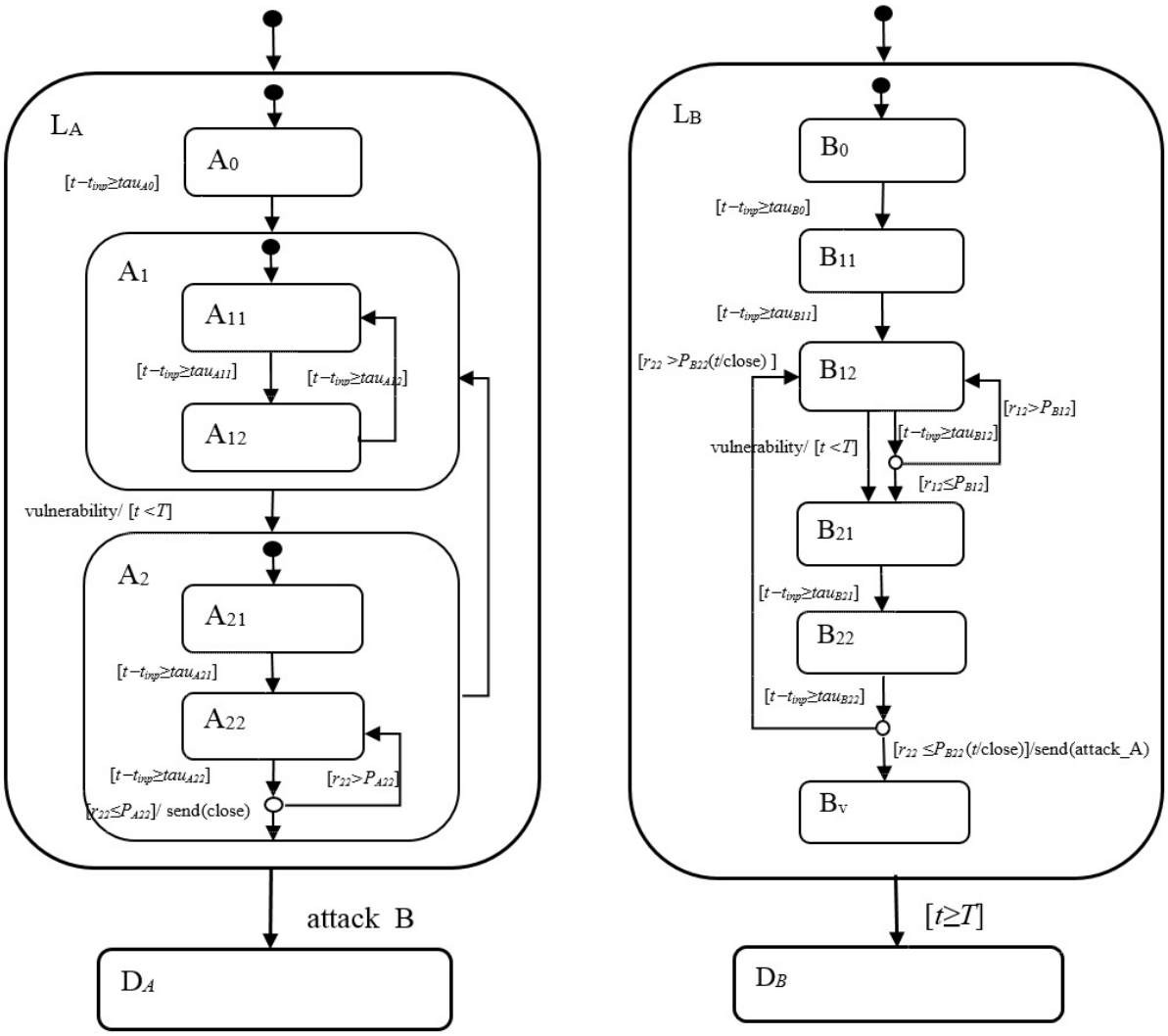


Рис. 1. Представление конфликтного взаимодействия систем с использованием гибридных автоматов

вало бы ввести все возможные переходы в D для внутренних состояний ГА АЭ.

Каждый АЭ в данной и подобных ей моделях [14, 15] определяется цепочкой последовательно выполняемых дискретных состояний с вероятностными или событийными переходами двух типов: в прямом направлении, задаваемом последовательностью дискретных состояний; в обратном направлении, подразумевающими возврат в предшествующее дискретное состояние для повторного выполнения работы на основе соответствующего типа локального поведения в этом состоянии. Можно показать, что любая последовательность действий в реальной системе может быть приведена к подобной схеме путем декомпозиции и/или агрегации в ней выполняемых работ.

Общий вид оператора локального поведения для любого состояния ГА АЭ (например, состояния A_k или состояния B_k) на интервале времени $[t_{k-1} = t_{inp},\ t_k = t_{out})$ в соответствии с [14, 15, 18] предлагается далее задавать на основе следующих соотношений:

$$x(t) = (\tau(t), r(t), u(t))^T = f(x(t_{k-1}), t),\ \ t_{k-1} = t_{inp},$$

$$x(t_{k-1}) = (\tau_k, r_k, t_{k-1} + \tau_k)^T, \qquad (4)$$

$$(\tau_k, r_k)^T:\ \ P_{A(B)k}(\tau, r) = P_{A(B)k}(r/\tau) P_{A(B)k}(\tau),$$

$$\tau(t) = \tau_k,\ \ r(t) = r_k,\ \ u(t) = u(t_{k-1}) - t,\ \ t \ge t_{k-1},$$

$$t_{out} = t_k = t : I(u(t) = 0),$$

где $x = (\tau, r, u)^T \in R^3$ вектор вещественных переменных, описывающих локальное поведение, причем τ – время выполнения работы для каждого дискретного состояния ГА АЭ;

r – переменная, характеризующая результат выполнения работы, которая может принимать как конечное число значений, так и значения на множестве континуум; u – переменная, являющаяся функцией времени и характеризующая интервал времени, остающийся до завершения работы и нахождения в данном состоянии; $P_{A(B)k}(\tau, r)$ – совместная плотность распределения τ и r, которые в общем случае являются статистически зависимыми случайными величинами. Система уравнений (4) определяет нахождение ГА АЭ в данном состоянии в интервале времени продолжительностью τ_k, значение которого генерируется на основе плотности распределения $P_{A(B)k}(\tau)$ при входе в данное состояние. Одновременно на основе условной плотности распределения $P_{A(B)k}(r/\tau_k)$ формируется значение r_k, определяющее достигаемый в процессе выполнения работы результат. Естественно, что во многих случаях достаточно использовать более упрощенное описание без учета вероятностного характера исхода, основываясь только на задании случайного времени выполнения работы.

Рассмотрим детальное описание АЭ каждой из сторон, которые в данном варианте конфликтного взаимодействия функционируют различным образом. Для АЭ стороны A при реализации способа событийного моделирования в рамках типизированного описания конфликта предлагается ввести следующие состоянии и переходы.

1. Множество $S_A^D = \{J_A\}$, состоящее из одной целочисленной переменной (индекс состояний) J_A, принимающей конечное множество значений, принадлежащих множеству символов дискретных состояний $J_a \in Q_A^L$;

2. Множество Q_A^L – символов, определяющих возможные дискретные состояния ГА АЭ и состоящее из следующих подмножеств $Q_A^L = Q_{A0}^L \cup Q_{A1}^L \cup Q_{A2}^L$.

Подмножество символов $Q_{A0}^L = \{A_0\}$ состоит из символа одного состояния, которое обозначает подготовительные действия для организации и приведения системы А в рабочее состояние (размещение и настройку «облачной» ИС, иначе «развертывание» А), которые выполняются однократно без возврата и повторения. Выход из A_0 определяется сторожевым условием вида $[t - t_{inp} \geq \tau_{A0}]$, задаваемым исходя из плотности распределения времени выполнении работы, определенной для этого состояния τ_{A0} : $P_{A0}(\tau)$.

Подмножество символов $Q_{A1}^L = \{A_{11}, A_{12}\}$ обозначает состояния активной деятельности системы в штатном режиме и являются вложенными для общего состояния A_1, которое трактуется как «система А защищена от всех известных ей уязвимостей». При этом A_{11} определяет состояние функционирования системы в штатном режиме, а состояние A_{12} – состояние проведения штатных регламентных работ (проверок, обновлений и т.п.). Выполнение переходов внутри A_1 определяется сторожевыми условиями вида $[t - t_{inp} \geq \tau_{A11}]$, $[t - t_{inp} \geq \tau_{A12}]$, задаваемыми исходя из плотностей распределения времени выполнении работ, определенных для каждого из этих состояний τ_k : $P_{Ak}(\tau)$.

Подмножество символов $Q_{A2}^L = \{A_{21}, A_{22}\}$ обозначает состояния деятельности системы в условиях возникновения (открытия) новой уязвимости. Они являются вложенными для общего состояния A_2, которое трактуется как «система А не защищена от открытой уязвимости». Здесь состояние A_{21} определяет состояние получения информации об уязвимости и ее анализ (включая задержку по времени, обусловленную как объективными, так и человеческими факторами). Состояние A_{22} определяет проведение работ по закрытию уязвимости на основе временного решения или решения предлагаемого поставщиком оборудования и программного обеспечения. Выполнение переходов внутри A_2 определяется сторожевыми условиями вида $[t - t_{inp} \geq \tau_{A21}]$, $[t - t_{inp} \geq \tau_{A22}]$, задаваемыми исходя из плотностей распределения времени выполнении работ, определенных для каждого из этих состояний $\tau_{A21} : P_{A21}(\tau)$, $\tau_{A22} : P_{A22}(\tau)$. Кроме того, после выхода из состояния A_{22} в точке ветвления разыгрывается вероятностное условие перехода в следующие состояния, которое определяется как $[r_{22} \leq P_{A22}]$ при успешном выполнении работы, и условие $[r_{22} > P_{A22}]$ возврата в A_{22} при неудачном исходе выполняемой работы. Здесь P_{A22} задаваемая в рам-

ках оператора локального поведения вероятность успешного выполнения работы при упрощенном описании исхода, когда в (4) $r(t) = r_k$ не зависит от времени.

3. Переход из агрегированного состояния A_1 в агрегированное состояние A_2 осуществляется под воздействием события vulnerability с условием, что эта уязвимость открывается на интервале времени $[t, T)$, отведенном для конфликтного взаимодействия систем. Для описания процесса возникновения уязвимостей может быть использована модель случайного потока событий, генерируемого из внешней среды. Гибридный автомат – источник (генератор) такого потока в схеме рис. 1 не представлен, чтобы не загромождать ее описание.

4. Переход из агрегированного состояния A_2 обратно в агрегированное состояние A_1 осуществляется при условии успешного завершения работ по закрытию уязвимости в A_2. На схеме рис. 1 этот переход осуществляется мгновенно после окончательного выхода из A_{22} и достижения границы A_2. При выполнении успешного выхода из A_{22} и, соответственно, из A_2 генерируется событие, сопровождающее этот переход: событие close (на рис. 1 обозначение *send*(close)), определяющее факт закрытия уязвимости.

Для АЭ стороны B при реализации событийного моделирования в рамках типизированного описания конфликта предлагается ввести следующие состояния и переходы.

1. Множество $S_B^D = \{J_B\}$, состоящее из одной целочисленной переменной (индекс состояний) J_B, принимающей конечное множество значений, принадлежащих множеству символов дискретных состояний $J_B \in Q_B^L$;

2. Множество Q_B^L – символов, определяющих возможные дискретные состояния ГА АЭ и состоящее из следующих подмножеств $Q_A^L = Q_{A0}^L \bigcup Q_{A1}^L \bigcup Q_{A2}^L$.

Подмножество символов $Q_{B0}^L = \{B_0\}$ состоит из символа одного состояния, которое обозначает подготовительные действия для организации и приведения системы В рабочее состояние («развертывание» В), которые выполняются однократно без возврата и повторения. Выход из B_0 определяется сторожевым условием вида $[t - t_{inp} \geq \tau_{B0}]$, задаваемым исходя из плотности распределения времени выполнении работы, определенной для этого состояния $\tau_{B0}: P_{B0}(\tau)$.

Подмножество символов $Q_{B1}^L = \{B_{11}, B_{12}\}$ обозначает группу состояний деятельности системы В в режиме поиска и обнаружения уязвимостей при нахождении системы А в состоянии A_1 (А защищена от всех известных ей уязвимостей). Состояние B_{11} здесь определяет функционирование системы, в рамках которого проводится сбор данных о системе А (анализ организационных принципов построения, используемых технических средствах и программном обеспечении, прав и квалификации пользователей и обслуживающего персонала). Состояние B_{12} определяет действия, направленные на поиск уязвимостей при работе А в штатном режиме. Выполнение перехода из B_{11} и B_{12} определяется сторожевыми условиями $[t - t_{inp} \geq \tau_{B11}]$, $[t - t_{inp} \geq \tau_{B12}]$, задаваемыми исходя из плотности распределения времени выполнения работ по сбору данных $\tau_{B11}: P_{B11}(\tau)$ и плотности распределения времени поиска уязвимостей $\tau_{B12}: P_{B12}(\tau)$. Кроме того, после выхода из состояния B_{12} в точке ветвления разыгрывается вероятностное условие перехода в следующее состояние, которое определяется как $[r_{12} \leq P_{B12}]$ при успешном выполнении работы, и условие $[r_{22} > P_{B12}]$ возврата в B_{12} при неудачном исходе. Здесь P_{B12} задается в рамках оператора локального поведения как вероятность успешного обнаружения уязвимости при функционировании А в штатном режиме и не зависит от времени. Уязвимости в применяемых технологиях могут быть обусловлены, в том числе, человеческим фактором (например, наличие прав при отсутствии квалификации пользователя даёт возможности нарушителю информационной безопасности по успешному применению методов социальной инженерии для получения неправомерного доступа к обрабатываемой в «облачной» ИС информации).

Помимо этого в модели, представленной на рис. 1, отображен еще один переход из B_{12} в следующую группу дискретных состояний. Он обусловлен воздействием события vulnerability (открытие новой уязвимости), возни-

кающего на интервале $[t,T)$. При этом принимается предположение, что информацию об открытии новой уязвимости системы А и В получают из внешней среды одновременно.

Следующее подмножество символов $Q^L_{B2}=\{B_{21},B_{22}\}$ обозначает состояния деятельности системы В после получения информации об обнаруженной тем или иным путем уязвимости. Здесь состояние B_{21} определяет действия, направленные на анализ обнаруженной уязвимости для ее использования и имеет конечное время (включая естественные задержки по времени, обусловленные как объективными, так и человеческими факторами). Состояние B_{22} определяет проведение действий по использованию уязвимости для нарушения безопасности использования облачной технологии в системе А. Выполнение переходов из B_{21}, B_{22} определяется сторожевыми условиями $[t-t_{inp}\ge\tau_{B21}]$, $[t-t_{inp}\ge\tau_{B22}]$, задаваемыми исходя из плотностей распределения времени $\tau_{B21}:P_{B21}(\tau)$, $\tau_{B22}:P_{B22}(\tau)$.

Кроме того, после выхода из состояния B_{22}, в точке ветвления разыгрывается вероятностное условие перехода в следующие состояния, которое определяется как $[r_{22}\le P_{B22}(t/\text{close})]$ при успешном выполнении работы, и условие $[r_{22}>P_{B22}(t/\text{close})]$ возврата в B_{12} при неудачном исходе выполняемой работы. Здесь P_{B22} задаваемая в рамках оператора локального поведения вероятность успешного выполнения работы уже зависит от времени и от возникновения события close (закрытие новой уязвимости в А).

Подмножество символов $Q^L_{Bv}=\{B_v\}$ состоит из символа одного состояния, называемого критическим состоянием (состоянием выигрыша). Переход в критическое состояние сопровождается созданием события attack_A, переводящего ГА стороны A из состояния L_A в собственное состояние D_A. Состояние B_v в данной модели является поглощающим.

3. Переход из состояния B_{22} обратно в состояние B_{12} осуществляется в случае неудачной попытки использования ранее обнаруженной уязвимости. Как уже отмечалось, условие перехода определяется вероятностью $P_{B22}(t/\text{close})$, которая зависит от того, насколько успешной и своевременной была деятельность А по закрытию уязвимости в состоянии A_2. Для определения этой вероятности как функции времени может использовано следующее соотношение:

$$P_{B22}(t/\text{close})=\begin{cases}P_{bv}, & t<t_{close},\\ 0, & t\ge t_{close},\end{cases}$$

где t_{close} – момент времени закрытия уязвимости в системе А; P_{bv} – вероятность использования стороной В имеющейся уязвимости при незащищенном режиме функционирования А. Если работы по закрытию уязвимости не проводилось, то устанавливается $t_{close}=T$.

Представленная модель конфликтного взаимодействия является типизированной и может уточняться и дополняться исходя из конкретной ситуации.

2. ОЦЕНКА НИЖНЕЙ ГРАНИЦЫ ДЛЯ ВЕРОЯТНОСТИ ВЫИГРЫША СТОРОН

Использование представленных выше моделей требует задания исходных данных и, прежде всего, задания вида плотностей распределения вероятностей для времени пребывания ГА в дискретных состояниях при реализации соответствующих локальных поведений. Этот вопрос в известной литературе неоднократно обсуждался [1, 14, 15], однако до сих пор не получил необходимых обоснований с точки зрения выбора вида таких распределений. Поэтому представляется целесообразным получения оценок вероятностей выигрыша, основанных на использовании самых общих параметров, таких, как математическое ожидание и дисперсия для времени пребывания в каждом дискретном состоянии или границ диапазонов возможных значений этого времени. Для проведения подобных оценок в данном случае достаточно определить моменты распределения времени перехода В в критическое состояние B_v. При этом целесообразно рассмотреть две ситуации, описываемые условными математическими ожиданиями и дисперсиями этого времени: ситуацию отсутствия открытия новой уязвимости на интервале $[0,T]$ – событие V и ситуация появления новой уязвимости на ин-

тервале $[0,T]$ – событие $\bar{V}$, известной обеим сторонам конфликта.

Изначально определим вероятности этих событий. Для определенности представим, что процесс появления уязвимостей описывается пуассоновским стационарным потоком событий с ограниченным последействием, имеющим плотность распределения интервала между событиями $f(\tau)=\lambda e^{-\lambda\tau}$. Тогда вероятности отсутствия и появления на интервале $[0,T]$ одной уязвимости определяются соотношениями:

$$P_T(\bar{V})=e^{-\lambda T}\approx 1-\lambda T,\ \ P_T(V)=\lambda T e^{-\lambda T}\approx \lambda T, \quad (5)$$

где λ интенсивность потока. Далее также будет использоваться предположение о том, что интенсивность потока уязвимостей не велика и вероятность появления более одной уязвимости мала по сравнению с вероятностями $P_T(\bar{V})$, $P_T(V)$.

Распределение времени появления t_o уязвимости на этом заданном интервале времени определяется соотношением:

$$P_T(t_o/V)=\frac{P_T(t_o,V)}{P_T(V)},$$

$$P_T(t_o,V)=\lambda(1-\int_0^{t_o} f(u)du)(1-\int_{t_o}^{T} f(u)du)=$$

$$=\lambda e^{-\lambda t_o}e^{-\lambda(T-t_o)}=\lambda e^{-\lambda T},$$

$$P_T(t_o/V)=\frac{P_T(t_o,V)}{P_T(V)}=\begin{cases}T^{-1}, t_o\in[0,T],\\ 0, \quad t_o\notin[0,T].\end{cases}$$

В итоге получен очевидный результат, свидетельствующий о равномерном распределении времени открытия уязвимости на интервале $[0,T]$.

2.1. Анализ вероятности выигрыша B без получения внешней информации о новой уязвимости

Запишем выражение для общего времени пребывания ГА АЭ B, в группе состояний $Q^L_{B0}\cup Q^L_{B1}\cup Q^L_{B2}=\{B_0,B_{11},B_{12},B_{21},B_{22}\}$, т. е. во всех состояниях за исключением критического при условии, что новая уязвимость не появилась (событие $\bar{V}$) и В работает в режиме обнаружения уязвимости собственными средствами. Это время как случайная величина определяется следующим соотношением:

$$\tau_{B,1}=\tau_{B0}+\tau_{B11}+\sum_{k=1}^{h_{22}}\sum_{s=1}^{h_{12,k}}\tau_{B12,k,s}+$$
$$+\sum_{k=1}^{h_{22}}\tau_{B21,k}+\sum_{k=1}^{h_{22}}\tau_{B22,k}, \quad (6)$$

где $h_{22}\in\{1,2,...,\infty\}$ – случайная величина, характеризующая количество циклов выполнения работ в группе состояний B_{21}, B_{12}, B_{22} с учетом возможности возврата (при $h_{22}>1$) после неудачной попытки использования ранее найденной уязвимости при отсутствии положительного результата на предыдущем цикле; $h_{12,k}\in\{1,2,...,\infty\}$ случайная величина, характеризующая количество циклов выполнения работ в состоянии B_{12} после неудачной попытки поиска уязвимости (при $h_{12,k}>1$) для k-го цикла выполнения группы работ в B_{21}, B_{12}, B_{22}; $\tau_{B12,k,s}$, $\tau_{B21,k}$, $\tau_{B22,k}$ – случайные длительности выполнения работ на s-м и k-м циклах повторения. Использование индекса k для случайной величины $h_{12,k}$ подчеркивает, что на разных циклах повторения B_{21}, B_{12}, B_{22} ее значение может быть различным, хотя формально в силу независимости h_{12}, h_{22} этого не требуется.

С учетом (6), считая заданными вероятности $P_{B12}=p_{bd}$, $P_{B22}=p_{bv}$ успешного завершения работы после пребывания в состояниях $B_{12}\in Q^L_{B1}$ $B_{22}\in Q^L_{B2}$, а также то, что случайные величины, определяющие время пребывания ГА АЭ в состояниях $Q^L_{B0}\cup Q^L_{B1}\cup Q^L_{B2}=\{B_{11},B_{12},B_{21},B_{22}\}$ независимы между собой, запишем выражение для условной (для рассматриваемого события $\bar{V}$ плотности распределения τ_b в виде h_{12}, h_{22}.

$$P_B(\tau_B/\bar{V})=P_{B1}(\tau_{B,1})=$$

$$=\sum_{\{h_{12},h_{22}\}}P(h_{12},h_{22})P_{B1}(\tau_{B.1}/h_{12},h_{22})=$$

$$=\sum_{h_{22}=1}^{\infty}\sum_{h_{12}=1}^{\infty}(1-p_{bd})^{h_{12}-1}p_{bd}(1-p_{bv})^{h_{22}-1}\times$$
$$\times p_{bv}P_B(\tau_{B,1}/h_{12},h_{22}). \quad (7)$$

В последнем выражении из (4) $P_{B1}(\tau_{B,1}/h_{12},h_{22})$ есть свертка плотностей распределения, описывающая композицию случайных величин (6) для условия, описываемого вектором $h=(h_{12},h_{22})^T$, каждая компо-

нента которого определяет количество повторяющихся циклов работы в соответствующих дискретных состояниях.

Для распределения вектора $h=(h_{12},h_{22})^T$ в (7) используется следующее представление, основанное на независимости компонентов вектора между собой и формуле для бесконечной геометрической прогрессии:

$$P(h_{12},h_{22})=P(h_{12})P(h_{22}),\ P(h_*)=(1-p_{b*})^{h_*-1}p_{b*},$$

$$\sum_{h_*=1}^{\infty}P(h_*)=\frac{p_{b*}}{1-(1-p_{b*})}=1. \qquad (8)$$

Выполнение расчетов на основе (7), (8) возможно только приближенно и только численными методами при наличии аналитического представления для каждой из используемых плотностей распределения времени. При этом формально для оценки вероятностей выигрыша для представленной схемы конфликта необходимо с использованием выражений для плотности $P_B(\tau_B/\bar{V})$ для стороны B определить вероятность

$$P_B^{(1)}=\Pr(\tau_{B,1}<T)=\int_0^T P_B(u/\bar{V})du. \qquad (9)$$

В итоге мы видим, что фактически в данном случае конфликт носит сугубо односторонний характер (В не взаимодействует и его исход не зависит от действий стороны А).

Рассмотрим теперь возможность использования фундаментальных неравенств теории вероятностей для получения граничных оценок для вероятности (9) на основе информации о первом и втором моментах распределения $P_{B1}(\tau_{B,1})=P_B(\tau_B/\bar{V})$. С этой целью определим условные математическое ожидание $m_{B,1}=M[\tau_{B,1}]$ и дисперсию $d_{B,1}=D[\tau_{B,1}]=$ $=M[(\tau_{B,1}-m_{B,1})^2]$ для $\tau_{B,1}$ на основе (6).

Используя (6)–(8), можно представить выражения для условного относительно $h=(h_{12},h_{22})^T$ математического ожидания $m_{B,1}(h)$ и безусловного математического ожидания $m_{B,1}$ следующим образом:

$$m_{B,1}(h)=M[\tau_{B,1}/h]=$$

$$=m_{B\tau 0}+m_{B\tau 11}+h_{22}h_{12}m_{B\tau 12}+h_{22}m_{B\tau 21}+h_{22}m_{B\tau 22}$$

$$m_{B,1}=M[\tau_{B,1}]=$$

$$=m_{B\tau 0}+m_{B\tau 11}+\frac{m_{B\tau 12}}{p_{bv}p_{bd}}+\frac{m_{B\tau 21}}{p_{bv}}+\frac{m_{B\tau 22}}{p_{bv}}. \qquad (10)$$

При получении (10) использовалось следующее преобразование для сумм бесконечным верхним пределом:

$$\sum_{h_*=1}^{\infty}h_*(1-p_{b*})^{h*-1}p_{b*}=$$

$$=p_{b*}\frac{d}{dp_{b*}}\left(-\sum_{h*=1}^{\infty}(1-p_{b*})^{h_*}\right)=$$

$$=p_{b*}\frac{d}{dp_{b*}}\left(-(1-p_{b*})\sum_{h_*=1}^{\infty}(1-p_{b*})^{h_*-1}\right)=$$

$$=p_{b*}\frac{d}{dp_{b*}}\left(-\frac{1-p_{b*}}{p_{b*}}\right)=\frac{1}{p_{b*}}.$$

Выражение для $d_{B,1}$ получим на основе следующих представлений. Введя сначала условную дисперсию для фиксированного вектора

$$d_{B,1}(h)=M[(\tau_{B,1}-m_{B,1})^2/h]=$$

$$=d_{B\tau 0}+d_{B\tau 11}+h_{22}h_{12}d_{B\tau 12}+h_{22}d_{B\tau 21}+h_{22}d_{B\tau 22}$$

и представляя безусловную дисперсию как:

$$d_{B,1}=M[(\tau_{B,1}-m_{B,1})^2]=$$

$$=\sum_{\{h_{12},,h_{22}\}}P(h_{12},h_{22})\int(\tau_{B,1}-m_{B,1})^2P(\tau_{B,1}/h_{12},h_{22})$$

окончательно получим:

$$d_{B,1}=d_{B\tau 0}+d_{B\tau 11}+\frac{d_{B\tau 12}}{p_{bv}p_{bd}}+\frac{d_{B\tau 21}}{p_{bv}}+\frac{d_{B\tau 22}}{p_{bv}}. \qquad (11)$$

Рассмотрим возможность получения оценок вероятностей выигрыша В при условии, что новая уязвимость не появилась (событие $\bar{V}$). В качестве первой из таких оценок, как и ранее в [14, 15], целесообразно рассмотреть гауссовское приближение для случайной величины $\tau_{b,1}$, учитывая, что в (6) выполняется суммирование независимых случайных величин, причем часть из этих слагаемых имеет одно и тоже распределение. Тогда такую оценку приближенно можно представить в виде:

$$P_{Bga}^{(1)}=\Pr(0<\tau_{B,1}<T)=\int_0^T N(u,m_{B,1},d_{b,1})du=$$

$$=F\left(\frac{T-m_{B,1}}{\sqrt{d_{B,1}}}\right)-F\left(\frac{-m_{B,1}}{\sqrt{d_{B,1}}}\right), \qquad (12)$$

$$F(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}N(v,0,1)dv.$$

где $N(u,m,d)$ – обозначение гауссовской плотности распределения вероятностей с соответствующими параметрами.

Помимо этого, целесообразно рассмотреть возможность получения других оценок на основе фундаментальных неравенств теории вероятностей. Для оценки вероятности события $\tau_{B,1} < T$ можно использовать неравенство Чебышева [21]. Пусть для определенности $m_{B,1} < T$. При этом, поскольку для исходного неравенства диапазон значений снизу не ограничен, можно записать следующее выражение для нижней границы вероятности выигрыша:

$$P_{Bch}^{(1)} = \Pr\left[\tau_{B,1} < T\right] = \\ = \Pr\left[\tau_{B,1} - m_{B,1} < T - m_{B,1}\right] \geq \\ \geq \Pr\left[\left|\tau_{B,1} - m_{B,1}\right| < T - m_{B,1}\right] \geq 1 - \frac{d_{B,1}}{\left(T - m_{B,1}\right)^2}. \quad (13)$$

Уточнить оценку $P_{Bch}^{(1)}$ в (13) можно, если предположить, что плотность распределения композиции $\tau_{b,1}$ является унимодальной. В подобном случае можно усилить результат (13) на основе использования неравенства Высочанского-Петунина [22]. С использованием этого неравенства может быть получена следующая нижняя граница для вероятности выигрыша:

$$P_{Bvp} = \Pr\left[\tau_{B,1} < T\right] \geq \Pr\left[\left|\tau_{B,1} - m_{B,1}\right| < T - m_{B,1}\right] = \\ = \Pr\left[\left|\tau_{B,1} - m_{B,1}\right| < \frac{T - m_{B,1}}{\sqrt{d_{B,1}}}\sqrt{d_{B,1}}\right] \geq \\ \geq 1 - \frac{4}{9\rho^2} = 1 - \frac{4d_{B,1}}{9(T - m_{B,1})^2}, \\ \rho = \frac{T - m_{B,1}}{\sqrt{d_{B,1}}} \geq \sqrt{\frac{8}{3}} = 1,6329. \quad (13)$$

Подобная оценка позволяет уточнить результат при достаточно больших значениях ρ, что вполне очевидно связано с необходимостью выбора соответствующей величины интервала времени T относительно $m_{B,1}$ $d_{B,1}$.

2.2. Анализ вероятности выигрыша B в режиме получения внешней информации о новой уязвимости

Существенно более сложной представляется задача оценки вероятности выигрыша B при условии, что на анализируемом интервале времени получена информация об открытии новой уязвимости (событие $\overline{V}$). Как и ранее, запишем выражение для общего времени пребывания ГА АЭ B в группе состояний $Q_{B0}^L \bigcup Q_{B1}^L \bigcup Q_{B2}^L = \{B_0, B_{11}, B_{12}, B_{21}, B_{22}\}$, т. е. во всех состояниях за исключением критического. Примем также допущение о том, что B приступает к использованию новой уязвимости в случае, если к моменту времени t_o выполнены все подготовительные работы в состояниях B_0, B_{11} или если к этому моменту времени не произошло использование самостоятельно найденной уязвимости. Тогда время до перехода в критическое состояние как случайная величина определяется следующими соотношениями:

$$\tau_{B,2} = \begin{cases} \tau'_{B,2} = \tau_{B0} + \tau_{B11} + \sum_{k=1}^{h_{22}} \sum_{s=1}^{h_{12,k}} \tau_{B12,k,s} + \\ \quad + \sum_{k=1}^{h_{22}} \tau_{B21,k} + \sum_{k=1}^{h_{22}} \tau_{B22,k}, \quad t_o \in \Omega_0, \\ \tau''_{B,2} = t_o + \tau_{B21} + \tau_{B22} + \\ \quad + h_c \left(\sum_{k=1}^{h_{22}} \sum_{s=1}^{h_{12,k}} \tau_{B12,k,s} + \sum_{k=1}^{h_{22}} \tau_{B21,k} + \right. \\ \quad \left. + \sum_{k=1}^{h_{22}} \tau_{B22,k} \right), \; t_o \in \Omega_1. \end{cases} \quad (14)$$

где τ_{B21}, τ_{B22} – интервалы, определяющие действия, выполняемые после открытия новой уязвимости в момент t_o в соответствующих состояниях. $h_c \in \{0,1\}$ – случайная величина, характеризующая факт использования ($h_c = 0$) появившейся в момент времени t_o уязвимости стороной B или перехода к стандартному циклу работ (поиск, анализ, использование) ($h_c = 1$), если эта уязвимость закрыта стороной A или стороне B не удалось ее использовать. Помимо этого, в (14) использованы следующие обозначения: $\Omega_0 = [0 < \tau_{B0} + \tau_{B11}] \bigcup [\tau'_{B,2}, T]$ – множе-

ство моментов времени, в которых новая уязвимость не используется; $t_o \in \Omega_1 = [\tau_{B0} + \tau_{B11},\ \tau'_{B,2}]$ – множество моментов времени, в которых новая уязвимость может использоваться. Все остальные обозначения в (14) по смыслу соответствуют обозначениям, ранее введенным в (6). Далее чтобы избежать зависимости границ интервалов Ω_0, Ω_1 от случайных величин, будем считать, что допустимые диапазоны значений времени перехода к использованию открытой извне уязвимости определяются детерминированным образом, например, исходя из математических ожиданий $m_I = \min(t_o) = M[\tau_{B0} + \tau_{B11}], m_A = \max(t_O) = M[\tau'_{B,2}]$.

В случае, если новая уязвимость не закрыта стороной А до истечения суммарного времени $\tau_{B21} + \tau_{B22}$, выполняется неравенство:

$$t_o + \tau_{B21} + \tau_{B22} < t_o + \tau_{A21} + \sum_{t=1}^{q_{22}} \tau_{A22,t}, \quad (15)$$

где $q_{22} \in \{1, 2, ..., \infty\}$ – случайная величина, характеризующая количество циклов выполнения работы в состоянии A_{22} с учетом возможности возврата (при $q_{22} > 1$) после неудачной попытки закрытия уязвимости при отсутствии положительного результата на предыдущем цикле.

При незакрытой уязвимости система В может воспользоваться этой ситуацией с вероятностью p_{bv}, близкой к единице, или с малой вероятностью $1 - p_{bv}$ осуществить возврат для проведения работ в стандартных циклах (поиск, анализ, использование). В случае если сторона А успевает закрыть уязвимость раньше, чем В ее использует однозначно $h_c = 1$ и осуществляется возврат для проведения работ в стандартных циклах с вероятностью, равной единице, что отражено в формуле (14).

С учетом этих соображений, получим выражения для плотности распределения времени $\tau_{B,2}$, а также первых двух моментов этого распределения при фиксированном значении t_o. Пусть $t_o \in \Omega_0$. Тогда, как следует из (14), распределение и моменты вычисляются по приведенным соотношениям (7)–(11). В частности, выражение для плотности распределения имеет вид:

$$\begin{aligned} P_B(\tau_B / V, t_o \in \Omega_0) &= P_{B2_1}(\tau'_{B,2} / t_o \in \Omega_0) = \\ &= \sum_{\{h_{12}, h_{22}\}} P(h_{12}, h_{22}) P_{B2}(\tau'_{B,2} / h_{12}, h_{22}) = \\ &= \sum_{h_{22}=1}^{\infty} \sum_{h_{12}=1}^{\infty} (1 - p_{bd})^{h_{12}-1} p_{bd} (1 - p_{bv})^{h_{22}-1} \times \\ &\times p_{bv} P_{B2}(\tau'_{B,2} / h_{12}, h_{22}). \end{aligned} \quad (16)$$

Пусть теперь $t_o \in \Omega_1$. Тогда, выражение для плотности распределения $\tau_{B,2}$ можно представить в виде:

$$\begin{aligned} P_B(\tau_B / V, t_o \in \Omega_1) &= P_{B2_2}(\tau''_{B,2} / t_o) = \\ &= P_{B22}(\tau''_{B,2} / v_a, t_o) P(v_a) + \\ &+ P_{B22}(\tau''_{B,2} / v_b, t_o) P(v_b),\ t_o \in \Omega_1, \\ P(v_a) &= \Pr(\delta_{ba} \geq 0),\ P(v_b) = \Pr(\delta_{ba} < 0), \\ \delta_{ba} &= \tau_{B21} + \tau_{B22} - \tau_{A21} + \sum_{t=1}^{q_{22}} \tau_{A22,t}, \end{aligned} \quad (17)$$

где v_a, v_b – обозначают события, соответствующие факту закрытия уязвимости стороной А до истечения суммарного времени $\tau_{B21} + \tau_{B22}$ в В и – факту нахождения А в незащищенном от этой уязвимости состоянии, а $P(v_a)$, $P(v_b)$ их вероятности. Очевидно, что, следуя (15), выполняется:

$$\begin{aligned} v_a &: \tau_{bv} = \tau_{B21} + \tau_{B22} \geq \tau_{av} = \tau_{A21} + \sum_{t=1}^{q_{22}} \tau_{A22,t} \\ v_b &: \tau_{bv} = \tau_{B21} + \tau_{B22} < \tau_{av} = \tau_{A21} + \sum_{t=1}^{q_{22}} \tau_{A22,t}. \end{aligned} \quad (18)$$

Неравенства (18) определяют конфликтный характер взаимодействия сторон А и В (сторона В должна завершить процесс использования открытой уязвимости раньше, чем ее закроет сторона А и наоборот). С учетом всех введенных обозначений для составляющих соотношений (17) можно получить следующее представление:

$$\begin{aligned} &P_{B22}(\tau''_{B,2} / v_a, t_o) = \\ &= \sum_{h_{22}=1}^{\infty} \sum_{h_{12}=1}^{\infty} (1 - p_{bd})^{h_{12}-1} p_{bd} (1 - p_{bv})^{h_{22}-1} \times \\ &\times p_{bv} P_{B2}(\tau''_{B,2} / v_a, h_c = 1, h_{12}, h_{22}, t_o), \end{aligned} \quad (19a)$$

$$\begin{aligned} &P_{B22}(\tau''_{B,2} / v_b, t_o) = \\ &= p_{bv} P_{B2}(\tau''_{B,2} = t_o + \tau_{B21} + \tau_{B22} / v_b, h_c = 0, t_o) + \end{aligned} \quad (19b)$$

$$+(1-p_{bv})\sum_{h_{22}=1}^{\infty}\sum_{h_{12}=1}^{\infty}(1-p_{bd})^{h_{12}-1}p_{bd}(1-p_{bv})^{h_{22}-1}\times$$
$$\times p_{bv}P_{B2}(\tau''_{B,2}/v_b, h_c=1, h_{12}, h_{22}, t_o),$$

В итоге на основе полученных соотношений можно оценить вероятность выигрыша для рассматриваемой ситуации при фиксированных границах областей Ω_0, Ω_1 для t_o как:

$$P_B^{(2)} = \Pr(\tau'_{B,2} < T / t_o \in \Omega_0)P(t_o \in \Omega_0) + \\ + \Pr(\tau''_{B,2} < T / t_o \in \Omega_1)P(t_o \in \Omega_1), \quad (20)$$

$$\Pr(\tau'_{B,2} < T / t_o \in \Omega_0) = \int_{t_o}^{T} P_{B2_2}(u / t_o \in \Omega_0)du,$$
$$\Pr(\tau''_{B,2} < T / t_o \in \Omega_1) =$$
$$= \Pr(\tau''_{B,2} < T / v_a, t_o \in \Omega_1)P(v_a) +$$
$$+ \Pr(\tau''_{B,2} < T / v_b, t_o \in \Omega_1)P(v_b) =$$
$$= \int_{\Omega_1}\frac{1}{V_{\Omega_1}}\int_{t_o}^{T} P_{B2_2}(u / t_0)dudt_o =$$
$$= \int_{\Omega_1}\frac{1}{V_{\Omega_1}}\int_{t_o}^{T}\left[P_{B22}(u / v_a, t_o)P(v_a) + \right.$$
$$\left. + P_{B22}(u / v_b, t_o)P(v_b)\right]dudt_o,$$
$$P(t_o \in \Omega_0) = V_{\Omega_0} \Big/ (V_{\Omega_0} + V_{\Omega_1}),$$
$$P(t_o \in \Omega_1) = V_{\Omega_1} \Big/ (V_{\Omega_0} + V_{\Omega_1}),,$$

где V_{Ω_0}, V_{Ω_1} – размеры областей Ω_0, Ω_1.

В (20) первое слагаемое для фиксированных Ω_0, Ω_1 рассчитывается или оценивается нижними границами так же, как и для события $\overline{V}$, на основе соотношений (7)–(15).

Второе слагаемое в (20) определяется с использованием распределений $P_{B22}(\tau''_{B,2}/v_a, t_o)$, $P_{B22}(\tau''_{B,2}/v_b, t_o)$, описываемых выражениями (14), (19a) и (19b). При получении гарантированных оценок вероятности выигрыша для $P_{B22}(\tau''_{B,2}/v_b, t_o)$ можно ввести определенные приближения, которые существенно упростят вычисления. Очевидно, что при $p_{bv} = 1-\varepsilon$, где $\varepsilon \geq 0$ малое число, выполняются неравенства:

$$P_{B22}(\tau''_{B,2}/v_b, t_o) \cong p_{bv}P_{B2}(t_o + \tau_{vb}/v_b, h_c = 0, t_o)$$

и слагаемым при сомножителе $1-p_{bv}$ при расчете этой плотности в (17b) можно пренебречь.

Также при вычислении соответствующей составляющей вероятности $\Pr(\tau''_{B,2} < T / v_b, t_o \in \Omega_1)$ в (20) для этой же плотности можно учесть, что в соответствие с (18) v_b: $\tau_{bv} < \tau_{av}$ и при вычислении второго интеграла использовать $P_{B2_2}(t_o + \tau_{va}/v_b, h_c = 0, t_o)$.

Расчет вероятностей событий $P(v_a) = \Pr(\delta_{ba} \geq 0)$, $P(v_b) = \Pr(\delta_{ba} < 0)$ может быть проведен стандартным образом на основе соотношений:

$$P(v_a) = \Pr(\tau_{av} \leq \tau_{bv}) = \int_{-\infty}^{\infty} P_{\tau av}(u)\left(\int_{u}^{\infty} P_{\tau bv}(v)dv\right)du, \quad (21)$$
$$P(v_b) = \Pr(\tau_{av} > \tau_{bv}) = \int_{-\infty}^{\infty} P_{\tau bv}(v)\left(\int_{u}^{\infty} P_{\tau av}(u)du\right)dv,$$

где $P_{\tau av}(u)$, $P_{\tau bv}(u)$ – соответствующие плотности распределении, получаемые как композиции плотностей для слагаемых в выражении для δ_{ba}

$$\delta_{ba} = \tau_{bv} - \tau_{av} = \tau_{B21} + \tau_{B22} - \tau_{A21} + \sum_{t=1}^{q_{22}}\tau_{A22,t}.$$

Таким образом, нами получена система вероятностных уравнений, обеспечивающих вычисление вероятности выигрыша стороной В при использовании определенных допущений и приближений. Для проведения этих вычислений, как и ранее, могут использоваться приближения для плотностей распределения композиций, неравенства, ограничивающие снизу вероятности выигрыша, а также прямые численные методы расчета.

3. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА И ИХ ОБСУЖДЕНИЕ

Другой подход, свободный от многих введенных допущений и приближений, основан на использовании технологий имитационного моделирования с применением представленных моделей, основанных на использовании формализма гибридных автоматов. Рассмотрим пример его реализации для задачи анализа вероятности выигрыша В. Проверка возможностей использования оценок (13)-(15), может быть проведена при использовании различных видов распределений $P_{Ak}(\tau_k)$, $k = \overline{1,m}$, $P_{Bk}(\tau_k)$, $k = \overline{1,m}$ для времени пребывания в состояниях подмножеств $Q^L_{Ad} \bigcup Q^L_{Ap} = \{A_1, ..., A_p, A_{p+1}, ..., A_m\}$ и $Q^L_{Bd} \bigcup Q^L_{Bp} = \{B_1, ..., B_p, B_{p+1}, ..., B_m\}$. Для реализации ИМ

с использованием формализма гибридных автоматов использовалась среда Matlab+ Simulink+Stateflow. Модель строилась с использованием трёх вложенных компонентов: главной программы, управляющей проведением статистического эксперимента (m-файл), запускаемой из него S-модели (Simulink-модели), являющейся оболочкой для объектной SF-модели (Stateflow-модели) и, собственно, самой – модели, реализующей представление объектов в виде карт состояний Харела (рис. 2) [20]. В рассмотренном выше примере структура реализованной SF-модели конфликта, как и в предыдущих главах в целом совпадает со структурой предложенной математической модели (рис. 1) и может быть однозначно понята исходя из стандартных обозначений среды.

Для множества статистических экспериментов, каждый из которых состоял из 1000 испытаний, рассматривались различные комбинации законов распределения, их параметров и вероятностей возврата для повторного выполнения работ. Для наглядности полученные результаты сведены к зависимостям вероятности выигрыша от отношения $\rho = (T - m_{B,1})^2 / d_{B,1}$. На рис. 3,а даны примеры типовых зависимостей для случая использования модели в режиме обнаружения уязвимостей собственными средствами, полученные при синхронном изменении вероятностей $p_{b12} = p_{b22}$ в диапазоне от 0,66 до

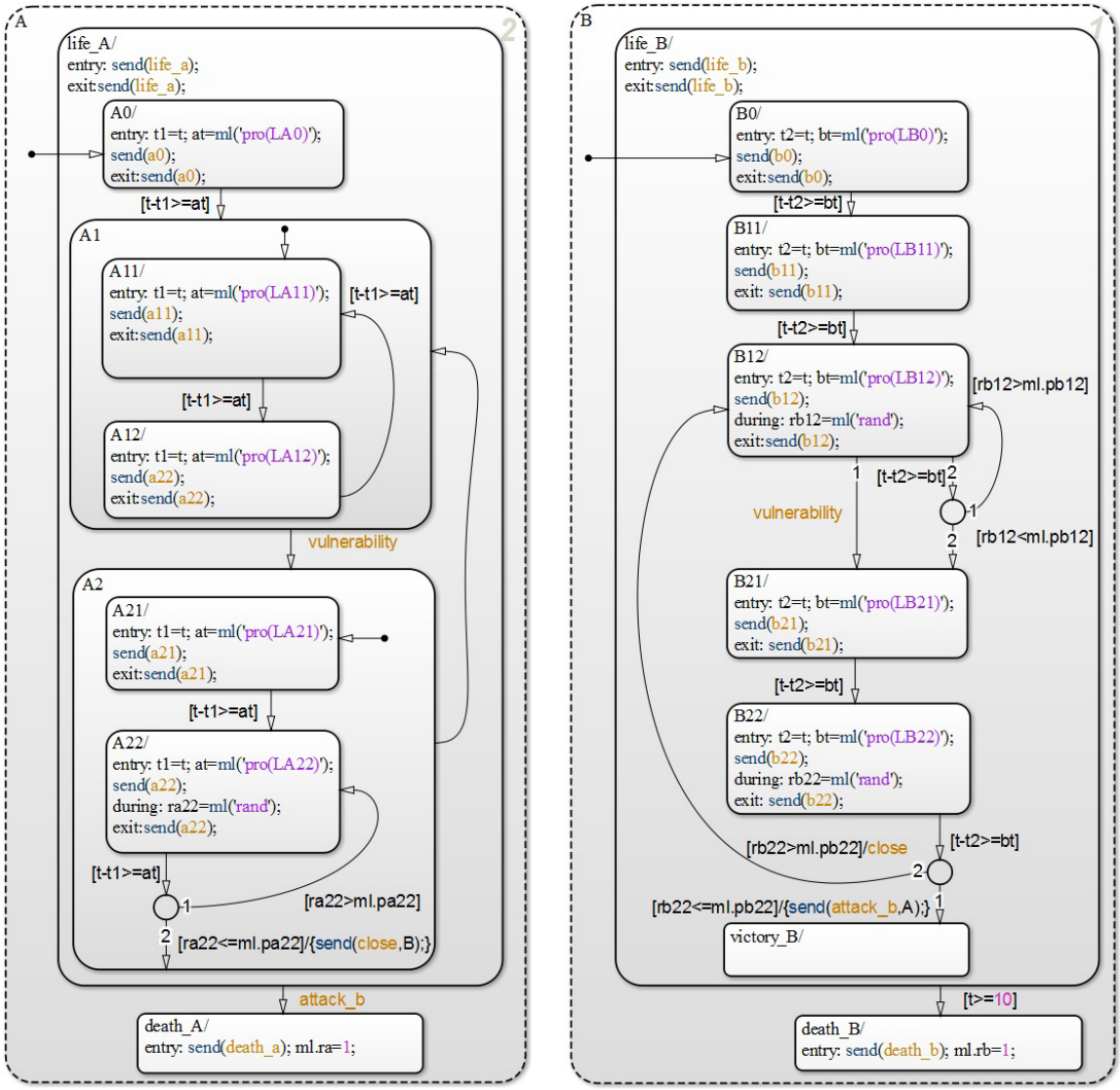
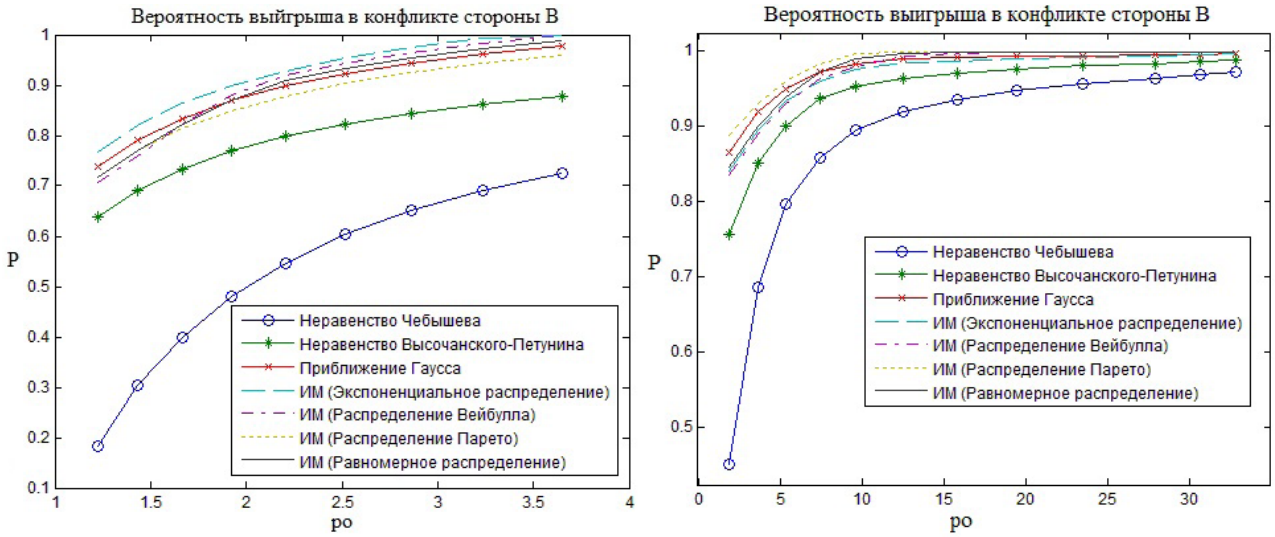


Рис. 2. Карты состояний для описания конфликта «облачной» информационной системы A и нарушителя безопасности информации B SF-модели конфликта



а) *б)*

Рис. 3. Результаты сравнения полученных оценок с результатами ИМ

0,79 с шагом 0.015. Математические ожидания и дисперсии для времени пребывания каждой из сторон в своих состояниях задавались одинаковыми $m_{ai}=m_{bi}=1,\ i=\overline{0,22}$ и $d_{ai}=d_{bi}=0.1,\ i=\overline{0,22}$ с одним и тем же законом распределения. На рис. 3,б приведены зависимости для случая использования описанной модели в режиме получения внешней информации о новой уязвимости, полученные для значений математического ожидания $m_{ai}=m_{bi},\ i=\overline{0,22}$ изменяющегося в диапазоне от 0,02 до 0,65 с шагом 0,055. При этом значения вероятностей для возвратных состояний задавались одинаковыми $p_{b12}=p_{b22}=0,7$. Дисперсии для времени пребывания в состояниях задавались равными $d_{ai}=d_{bi}=0,1,\ i=\overline{11,22}$. Эксперименты проводились при одном и том же законе распределения.

Анализ представленных зависимостей показывает, что достаточно точной оказалась оценка, полученная на основе неравенства Высочанского – Петунина, а также оценка, основанная на гауссовском приближении. Физический смысл полученных зависимостей состоит в том, что чем больше значение параметра ρ, характеризующего относительное среднестатистическое различие между общим временем рассмотрения конфликта и временем, необходимым для нарушения безопасности информации, тем больше вероятность нарушения безопасности информации в «облачной» информационной системе. Это говорит о важности фактора времени при реализации упреждающего характера воздействия по сравнению с вероятностью «поражения» на конечных этапах поиска уязвимостей в «облачной» информационной системе и их использования.

ЗАКЛЮЧЕНИЕ

Предложенные типовые концептуальная и математическая модели несимметричных конфликтных взаимодействий информационной системы, построенной с использованием «облачных» технологий и нарушителя безопасности информации, актуальны к применению в задачах исследования безопасности информационных систем и технологий. Обоснованные модели возможно и целесообразно использовать как базовые для составления более сложных моделей в интересах исследования возникающих на практике ситуаций.

Полученные для несимметричных конфликтных взаимодействий «облачной» информационной системы и нарушителя безопасности информации аналитические соотношения на основе приближения Гаусса, неравенства Чебышева и неравенства Высочанского-Петунина позволяют проводить оценку вероятности нарушения безопасности информации в условиях неопределённости вида плотностей распределений для времени

пребывания сторон в своих возможных состояниях. Однако, при возрастании сложности моделей их аналитическое описание требует высоких временных и трудовых затрат. В таком случае, кардинальное решение задачи исследования закономерностей конфликта лежит, главным образом, в применении технологий имитационного моделирования с использованием объектно-ориентированного подхода.

СПИСОК ЛИТЕРАТУРЫ

1. *Макаренко, С. И.* Информационные конфликты – анализ работ и методологии исследования / С. И. Макаренко, Р. Л. Михайлов // Системы управления, связи и безопасности. –2016. – № 3. – С. 95–178.

2. *Козирацкий, Ю. Л.* Модели информационного конфликта средств поиска и обнаружения / Ю. Л. Козирацкий // Радиотехника. – 2013. – 232 с.

3. *Дружинин, В. В.* Введение в теорию конфликта / В. В. Дружинин, А. С. Конторов, Д. С. Конторов. – М. : Радио и связь, 1989. – 288 с.

4. *Сухоруков, Ю. С.* Принципы моделирования динамики взаимодействия сторон в условиях радиолокационного конфликта / Ю. С. Сухоруков, В. М. Шляхин // Радиотехника. – 1992. – №1-2. – С. 44–59.

5. *Будников, С. А.* Оценка вероятностных показателей в конфликте информационно-управляющих систем. / С. А. Будников // Системы управления и информационные технологии. Научно-практический журнал. – 2009. – №3(37). – С. 27–31.

6. *Радько, Н. М.* Динамическая модель работы адаптированного к помехам радиосредства с использованием сетей Петри / Н. М. Радько, А. Н. Мокроусов // Информация и безопасность. – 2009. – № 2. – С. 257–262.

7. *Семисошенко, М. А.* Управление автоматизированными сетями декаметровой связи в условиях сложной радиоэлектронной обстановки / М. А. Семисошенко. – СПб. : ВАС, 1997. – 364 с.

8. *Губанов, Д А.* Социальные сети: модели информационного влияния, управления и противоборства / Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили // Под ред. Д.А. Новикова. – М. : Издательство физико-математической литературы, 2010. – 228 с.

9. *Коцыняк, М. А.* Обеспечение устойчивости информационно-телекоммуникационных систем в условиях информационного противоборства / М. А. Коцыняк, А. И. Осадчий, М. М. Коцыняк, О. С. Лаута, В. Е. Дементьев, Д. Ю. Васюков. – СПб. : ЛО ЦНИИС, 2015. – 126 с.

10. *Вакуленко, А. А.* Математическая модель динамики конфликта радиоэлектронных систем / А. А. Вакуленко, В. И. Шевчук // Радиотехника. – 2011. – № 1. – С. 56–59.

11. *Радзиевский, В. Г.* Информационное обеспечение радиоэлектронных систем в условиях конфликта / В. Г. Радзиевский, А. А. Сирота – М. : ИПРЖР, 2001. – 456 с.

12. *Андреещев, И. А.* Полумарковская модель оценки конфликтной устойчивости информационной инфраструктуры / И. А. Андреещев, С. А. Будников, А. В. Гладков // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2017. – № 1. – С. 10–17.

13. *Вялых, А. С.* Оценка уязвимости информационной системы на основе ситуационной модели динамики конфликта / А. С. Вялых, С. А. Вялых, А. А. Сирота // Информационные технологии. – 2012. – № 9. – С. 16–21.

14. *Сирота, А. А.* Моделирование конфликтного взаимодействия систем с использованием формализма гибридных автоматов / А. А. Сирота, Н. И. Гончаров // Информационные технологии. – 2018. – Т. 24, № 1. – С. 17–27.

15. *Сирота, А. А.* Исследование конфликта коалиций систем с использованием формализма гибридных автоматов / А. А. Сирота, Н. И. Гончаров // Вестник Воронеж. гос. ун-та. Сер. Системный анализ и информационные технологии. – 2017. – № 4. – С. 56–70.

16. *Алгазинов, Э. К.* Анализ и компьютерное моделирование информационных процессов и систем / Э. К. Алгазинов, А. А. Сиро-

та. – Под общ. ред. д.т.н. А. А. Сироты. – М. : Диалог-МИФИ, 2009. – 416 с.

17. *Колесов, Ю. Б.* Моделирование систем. Динамические и гибридные системы. Учебное пособие. / Ю.Б. Колесов, Ю.Б. Сениченков. – СПб. : БХВ-Петербург, 2012. – 224 с.

18. *Шпаков, В. М.* Ситуационные спецификации имитационных моделей гибридных реактивных систем / В. М. Шпаков // Труды СПИИРАН. – 2002. – Вып. 1, Т. 2. – С. 212–222.

19. *Парийская, Е. Ю.* Сравнительный анализ математических моделей и подходов к моделированию и анализу непрерывно-дискретных систем / Е. Ю. Парийская // Дифференциальные уравнения и процессы управления. – 1997. – № 1. – С. 91–120.

20. *Harel, D.* Statechars: a Visual Formalism for complex systems / D. Harel // Science of Computer Programming. – 1987. – V. 8. – P. 231–274.

21. *Колмогоров, А. Н.* Элементы теории функций и функционального анализа / А. Н. Колмогоров, С. В. Фомин. – Изд. четвёртое, переработанное. – М. : Наука, 1976. – 544 с.

22. *Высочанский, Д. Ф.* Обоснование правила 3-sigma для одномодальных распределений / Д. Ф. Высочанский, Ю. И. Петунин // Теория вероятностей и мат. статистика. – 1979. – Вып. 21. – С. 23–35.

Сирота Александр Анатольевич – д-р техн. наук, профессор, заведующий кафедрой технологий обработки и защиты информации Воронежского государственного университета.
E-mail: sir@cs.vsu.ru;

Гончаров Никита Игоревич – ассистент кафедры технологий обработки и защиты информации Воронежского государственного университета.
E-mail: goncharov_n_i@cs.vsu.ru.

Sirota Alexander Anatolievich – Doctor of Technical Sciences, Professor, Head of the Department of Information Processing Technologies and Information Protection of Voronezh State University.
E-mail: sir @ cs. vsu.ru

Goncharov Nikita Igorevich – assistant of the Department of Information Processing Technologies and Information Protection of Voronezh State University.
E-mail: goncharov_n_i@cs.vsu.ru