УДК 004.056.53

К. А. Щеглов, аспирант, **А. Ю. Щеглов,** д-р техн. наук, проф., e-mail: info@npp-itb.spb.ru
Университет ИТМО, Санкт-Петербург, Россия

Вопросы корректности и универсальности подхода к моделированию надежностных параметров и характеристик угроз атак

Исследованы вопросы корректности и универсальности предложенного подхода к моделированию угроз атак, позволяющего определять надежностные параметры и характеристики угрозы атаки. Подход основан на построении марковской модели угрозы атаки — модели с дискретными состояниями и непрерывным временем, с последующим ее преобразованием в модель вероятностного разрежения входных потоков случайных событий. Исследование, проведенное на модели вероятностного разрежения входных потоков случайных событий, позволило сделать вывод о том, что марковская модель с дискретными состояниями и непрерывным временем без потерь должна быть счетной (не конечной), и о том, что применение подобной модели корректно для решения задачи моделирования угроз атак. Предложен подход к формированию допущений для преобразования счетной марковской модели в конечную с использованием закона Пуассона. Исследованы вопросы универсальности предложенного подхода к моделированию угроз атак, достигаемой за счет реализации предложенного подхода к объединению состояний в модели вероятностного разрежения входных потоков случайных событий.

Ключевые слова: *угроза атаки, угроза уязвимости, резервирование, нивелирование, математическое моделирование, параметр и характеристика безопасности, надежность информационной безопасности, количественная мера актуальности угрозы атаки, марковская модель, разрежение входных потоков случайных событий*

Введение

В работах [1, 2] изложен метод моделирования угрозы атаки марковской моделью с дискретными состояниями и непрерывным временем без потерь, основанный на введенной в [3] интерпретации угрозы атаки[1]схемой параллельного резервирования создающих ее угроз уязвимостей[2]. В результате моделирования могут быть рассчитаны надежностные параметры и характеристики угрозы атаки, которые могут использоваться для количественной оценки уровня ее актуальности при принятии решения о необходимости в отношении нее реализации защиты. Искомые параметры и характеристики угрозы атаки названы нами "надежностными", поскольку при этом моделируется не атака, как процесс последовательного деструктивного воздействия нарушителем на систему [4—8], а именно угроза атаки, как процесс возникновения и устранения в системе отказов информационной безопасности — реальных угроз атак, создаваемых возникающими в системе реальными угрозами уязвимостей. Как следует из ГОСТ 27.002—89 "Надежность в технике. Основные понятия. Термины и определения", надежность — это свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования. Исходя из данного определения и проводя моделирование в рамках предложенной интерпретации угрозы атаки, можем говорить об определении надежностных параметров и характеристик безопасности информационной системы, а в общем случае — о свойстве надежности информационной безопасности, под которой понимаем свойство информационной системы сохранять во времени в установленных пределах значения всех характеристик безопасности, определяющих способность выполнять требуемые функции в безопасном режиме. А вот построение и включение в модель угрозы атаки математической модели нарушителя [2] уже позволяет получать необходимые при проектировании системы защиты информации эксплуатационные параметры и характеристики безопасности, в данном случае — реализации возникающей в информационной системе реальной угрозы атаки потенциальным нарушителем, поскольку в данной модели уже учитывается сложность реализации угрозы атаки и готовность потенциального нарушителя к реализации реальной угрозы атаки в целях получения несанкционированного доступа к информации, представляющей для него определенную ценность.

В [1] дано обоснование корректности использования марковских процессов (процессов без последействия) для моделирования угрозы атаки при предложенной ее интерпретации, в [2] рассмотрена возможность использования с этой целью конечных (конечное число состояний) марковских моделей с дискретными состояниями и непрерывным временем (конечные непрерывные цепи Маркова) без потерь, однако не исследованы вопросы кор-

[1] Под угрозой атаки понимаем угрозу безопасности, создаваемую совокупностью угроз уязвимостей, реализация которых потенциальным нарушителем необходима для осуществления этой атаки. Под реальной угрозой атаки понимаем условие, при котором все уязвимости, необходимые для реализации этой атаки, одновременно присутствуют в информационной системе — все угрозы уязвимостей, создающие угрозу этой атаки, реальны.

[2] Под угрозой уязвимостей понимаем угрозу возникновения (присутствия) свойства информационной системы, обусловливающего возможность реализации на нее атаки потенциальным нарушителем.

ректности применения для решаемых задач моделирования данного математического аппарата. Проведем данные исследования в этой работе.

Подход к моделированию угрозы атаки и проблема корректности используемой марковской модели

Прежде всего, уточним, что в [9] была введена классификация угроз уязвимостей, которые в общем случае могут быть отнесены к технологическим — безусловным или условным, это уязвимости, связанные с некорректностью реализации защиты, и к уязвимостям реализации, в первую очередь, это ошибки программирования[3]. Угрозы технологических уязвимостей, в том числе условных, возникающих при выявлении уязвимости реализации, должны нивелироваться системами защиты информации, что можно позиционировать как постановку задачи защиты информации от несанкционированного доступа в общем виде [9]. А вот угрозы уязвимостей реализации[4], которые с какими-то интенсивностями возникают и устраняются в системе, должны рассматриваться при моделировании угрозы атаки.

Очень важным, как увидим далее, является то, что, как показано в [1], следует говорить не об угрозах уязвимостей реализации, а об угрозах уязвимостей реализации соответствующего типа, предполагая при этом возможность одновременного (не одномоментного) появления в системе нескольких угроз уязвимостей одного типа. При этом под угрозами уязвимостей реализации одного типа понимаем угрозы реализации, создающие угрозу атаки на одну и ту же условную технологическую уязвимость.

Исходными данными при моделировании выступают интенсивность возникновения уязвимости λ и интенсивность устранения уязвимости μ, которые могут быть объективно, без использования каких-либо экспертных оценок, определены из соответствующей статистики [1]. Задачей же моделирования является определение параметров и характеристики безопасности угрозы атаки, создаваемой соответствующей совокупностью (набором) угроз уязвимостей реализации, таких как интенсивность возникновения и устранения в системе реальной угрозы атаки (λ_a и μ_a), вероятности готовности к безопасной эксплуатации информационной системы в отношении угрозы атаки (P_{0a}), среднего времени наработки на отказ безопасности информационной системы (восстанавливаемая система) в отношении угрозы атаки ($T_{0y.a}$), среднего времени восстановления безопасности информационной системы ($T_{в.у.а}$) в отношении угрозы атаки, которые могут рассматриваться в качестве количественных оценок (меры) актуальности угрозы атаки при последующем проектировании системы защиты.

Подход к моделированию угрозы атаки [2] состоит в построении конечной марковской модели с дискретными состояниями и непрерывным временем с последующим приведением построенной марковской модели угрозы атаки к модели вероятностного разрежения входных потоков случайных событий и расчетом на ней требуемых параметров и характеристик угрозы атаки.

Проиллюстрируем данный подход к моделированию на примере. Пусть угроза атаки создается двумя угрозами (типами угроз) уязвимостей реализации (исключили из рассмотрения соответствующие угрозы технологических уязвимостей), с соответствующими их параметрами — интенсивностями выявления и устранения уязвимостей (аналогичным образом можно построить модель для угрозы атаки любой сложности). Состояния системы обозначим через S_{ij}, где i — число выявленных уязвимостей первого типа, j — число уязвимостей второго типа. Размеченный граф системы состояний случайного процесса (марковского процесса) приведен на рис. 1, *а*.

Построение модели вероятностного разрежения входных потоков основано на следующих соображениях. Входной поток событий, поступающий в систему (на вход марковской модели), вероятностно разрежается — распределяется между состояниями системы в том смысле, что событие может наступить в случайный момент времени, когда система находится в одном из возможных своих состояний (переходы между состояниями в марковской модели осуществляются мгновенно).

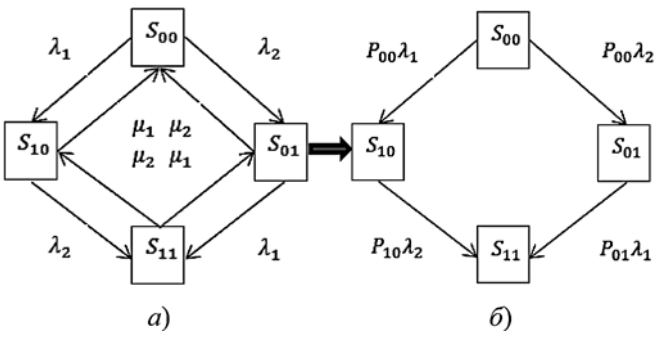

Рис. 1. Иллюстрация преобразования размеченного графа системы состояний случайного процесса марковской модели:
а — марковская модель; *б* — модель вероятностного разрежения входных потоков

[3] Под угрозой технологических уязвимостей понимаем технологические недостатки построения информационной системы в части обеспечения безопасности информации, включая отсутствие требуемых функций защиты информации, либо некорректность их реализации, не позволяющие в полном объеме реализовать защиту от несанкционированного доступа к информации. Под угрозой безусловной технологической уязвимости понимаем угрозу технологической уязвимости, присутствующую в информационной системе всегда — без возникновения каких-либо дополнительных условий. Данная угроза всегда реальна. Под угрозой условной технологической уязвимости понимаем угрозу технологической уязвимости, которая создается (становится реальной) в информационной системе при возникновении неких дополнительных условий, без которых соответствующая штатная возможность системы не несет в себе угрозы безопасности информации.

[4] Под угрозой уязвимостей реализации понимаем ошибки реализации (программирования) используемых в информационной системе средств или некоторые штатные возможности системных средств и/или приложений, создающие условия возникновения в системе реальной угрозы условной технологической уязвимости.

Важнейшее свойство входного потока случайных событий, которое требуется учитывать при моделировании угрозы атаки, — это его стационарность, поскольку очевидно, что уязвимости в системе возникают в случайные моменты времени, какая-либо регулярность данного потока отсутствует. С учетом выполнения свойства ординарности и отсутствия последействия [1], примем при моделировании, что входной поток случайных событий простейший (стационарный пуассоновский), что далее будем учитывать при анализе корректности моделей.

Получим из модели, приведенной на рис. 1, *а*, модель вероятностного разрежения входных потоков (рис. 1, *б*). При этом будем исходить из того, что вероятностное разрежение простейшего потока событий, при котором любое событие случайным образом с некоторой вероятностью p исключается из потока независимо от того, исключены другие события или нет, приводит к образованию простейшего потока с интенсивностью $\lambda' = p\lambda$, где λ — интенсивность исходного потока. Поток исключенных событий — тоже простейший с интенсивностью $\lambda'' = (1 - p)\lambda$ [10].

Замечание. В данном случае мы рассматриваем не исключение событий из потока, что реализуется в системах с потерями [10], а их распределение между состояниями системы — вероятностное разрежение входных потоков между возможными состояниями системы S_{ij}. В данном случае моделируется система без потерь, так как каждая возникающая в системе уязвимость реализации должна непременно устраняться.

При построении данной модели будем исходить из того, что вероятность нахождения системы в каком-либо состоянии в исходной марковской модели с дискретными состояниями и непрерывным временем (см. рис. 1, *а*), интерпретируется как доля времени нахождения системы в этом состоянии. Естественно, можно утверждать, что входной поток — поток, поступающий на вход модели с интенсивностью λ, распределятся между состояниями системы S_{ij} пропорционально P_{ij} — вероятностям нахождения системы в состояниях S_{ij}, определяемым для исходной марковской модели. С учетом этого получаем модель, приведенную на рис. 1, *б*.

Принципиальное отличие данной модели от марковской модели состоит в том, что переходы между состояниями на этой модели "взвешиваются" (размечаются) не интенсивностями возникновения событий в системе, а интенсивностями соответствующих вероятностно разреженных потоков — интенсивностями переходов между состояниями.

Для обоснования корректности данного преобразования достаточно построить модель вероятностного разрежения потоков (всех потоков, не только входных) в системе (рис. 2).

Как видим, обозначив через P_{ij} вероятность нахождения системы в состоянии S_{ij}, можем для обеих

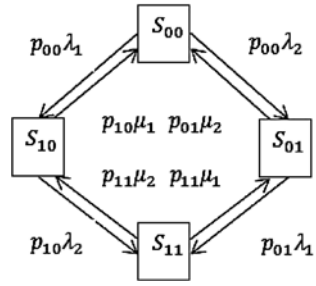

Рис. 2. Модель полного вероятностного разрежения потоков в системе

моделей, представленных на рис. 1, *а* и на рис. 2, записать одну и ту же систему линейных уравнений, что подтверждает корректность модели вероятностного разрежения входных потоков случайных событий:

$$\begin{cases} \mu_1 P_{10} + \mu_2 P_{01} = (\lambda_1 + \lambda_2) P_{00}; \\ \lambda_1 P_{00} + \mu_2 P_{11} = (\lambda_2 + \mu_1) P_{10}; \\ \lambda_2 P_{00} + \mu_1 P_{11} = (\lambda_1 + \mu_2) P_{01}; \\ \lambda_2 P_{10} + \lambda_1 P_{01} = (\mu_1 + \mu_2) P_{11}, \end{cases}$$

решая которую, с учетом полной группы событий, т.е. используя условие

$$P_{00} + P_{01} + P_{10} + P_{11} = 1,$$

находим искомые предельные (или финальные) вероятности состояний.

С использованием модели вероятностного разрежения входных потоков параметр безопасности угрозы атаки λ_a может быть рассчитан по следующей формуле:

$$\lambda_a = \sum_{S_i \in S_{(R-1)}} P_{S_i} \lambda_{S_i, S_R},$$

где $S_{(R-1)}$ — множество состояний системы, характеризуемых отсутствием в системе реальной угрозы атаки (не все создающие угрозу атаки уязвимости выявлены и устранены), в каждом из которых система находится с вероятностью $P_{S_{(R-1)}}$, S_R — состояние возникновения в системе реальной угрозы атаки (все создающие угрозу атаки уязвимости выявлены, но не устранены). В состояние S_R из состояний $S_{(R-1)}$ в системе осуществляется переход с интенсивностью $\lambda_{S_{(R-1)}, S_R}$.

Например, для модели, представленной на рис. 1, *б*, λ_a определяется следующим образом:

$$\lambda_a = P_{10}\lambda_2 + P_{01}\lambda_1.$$

Очевидно, что в стационарном (установившемся) режиме функционирования системы за долю времени нахождения системы в состоянии, характеризуемом возникновением реальной угрозы атаки, определяемой, как $1 - P_{0a}$, где P_{0a} — это вероятность готовности системы к безопасной эксплуатации в отношении угрозы атаки, из состояния, характеризующего реальную угрозу атаки, исходит поступающий

в него поток событий интенсивностью λ_a (система без потерь, все выявляемые уязвимости устраняются). Сказанное позволяет рассчитывать параметр безопасности μ_a угрозы атаки следующим образом:

$$\mu_a = \frac{\lambda_a}{1 - P_{0a}}.$$

Для рассматриваемого примера имеем:

$$\mu_a = \frac{P_{10}\lambda_2 + P_{01}\lambda_1}{P_{11}}.$$

Соответствующим образом можем определить и характеристики безопасности угрозы атаки.

Вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозы атаки:

$$P_{0a} = P_{00} + P_{10} + P_{01} = \frac{\mu_1\mu_2 + \lambda_1\mu_2 + \lambda_2\mu_1}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)},$$

среднее временя наработки на отказ безопасности информационной системы (восстанавливаемая система) в отношении угрозы атаки $T_{0у.а}$, среднее время восстановления безопасности информационной системы $T_{в.у.а}$ в отношении угрозы атаки:

$$T_{в.у.а} = \frac{1}{\mu_a},\ T_{0.у.а} = \frac{1}{\lambda_a} - T_{в.у.а}. \qquad (1)$$

Замечание. Следуя модели, представленной на рис. 1, *а*, отношением $1/\lambda_a$ определяется характеристика среднего времени наработки системы между отказами безопасности, равного $T_{0у.а} + T_{в.у.а}$.

Отметим, что подобным образом может быть построена математическая модель угрозы атаки, создаваемой любым числом угроз (типов угроз) уязвимостей реализации, например, для случая, когда угроза атаки создается тремя угрозами уязвимостей реализации, модель представлена на рис. 3.

На графе представлены следующие возможные состояния системы: S_0 — исходное состояние системы, S_i — в системе возникла и не устранена одна из уязвимостей реализации (на тип выявленной уязвимости указывает индекс), S_{ij} — в системе возникли и не устранены одновременно две уязвимости, S_{iji} — в системе возникли и не устранены одновременно все три уязвимости.

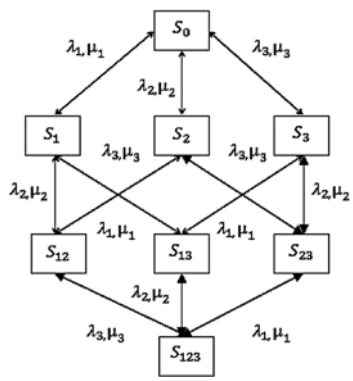

Рис. 3. Размеченный граф системы состояний случайного процесса для угрозы атаки, создаваемой тремя угрозами уязвимостей реализации

Теперь рассмотрим проблему использования для моделирования угрозы атаки конечной (с конечным числом состояний) марковской модели с дискретными состояниями и непрерывным временем. Именно такие модели приведены на рис. 1, *а* и рис. 3. Исследовать данную проблему нам позволит модель вероятностного разрежения входных потоков.

Замечание. Если число возможных состояний конечно или счетно (всем возможным состояниям могут быть присвоены порядковые номера), то случайный процесс называется процессом с дискретными состояниями [11].

Модель с конечным числом состояний нам необходима, так как требуется анализировать интенсивности переходов между определенными состояниями, набор которых в модели должен быть конечным.

Определим, например, интенсивность потока событий, циркулирующего в модели вероятностного разрежения входных потоков, создаваемого возникновением и устранением первого типа уязвимостей (см. рис. 1). На вход модели для этой угрозы уязвимостей поступает соответствующий простейший поток событий с интенсивностью λ_1. Этот поток событий переводит систему из состояния S_{00}, в котором система находится с вероятностью P_{00}, и из состояния S_{10}, в котором система находится с вероятностью P_{10}, т.е. вероятностно разрежается между двумя состояниями системы S_{00} и S_{01}. Как следствие, интенсивность рассматриваемого потока событий, циркулирующего в модели, обозначим ее $\lambda_{п1}$ определяется следующим образом:

$$\lambda_{п1} = (P_{00} + P_{01})\lambda_1 < \lambda_1,$$

Вызвано данное противоречие ($\lambda_{п1} < \lambda_1$) тем, что не из всех состояний марковской модели есть переходы, создаваемые потоком событий с интенсивностью λ_1, поступающим на вход марковской модели — переходы отсутствуют для состояний S_{10} и S_{11}, входной поток разрежается не между всеми состояниями, т.е. в системе присутствуют интервалы времени, в течение которых события в систему не поступают, что в общем случае уже не позволяет говорить о корректности использования для такой модели простейшего (стационарного пуассоновского) входного потока случайных событий. Естественно, используя подобную модель, имеем погрешность моделирования, которая применительно к рассматриваемому примеру тем больше, чем больше значение суммы $P_{10} + P_{11}$ (в общем случае — это сумма значения вероятностей состояний, из которых не выходит анализируемый поток событий). В нашем случае — при моделировании угроз атак — погрешность моделирования, вызванная рассматриваемой проблемой, может быть достаточно большой, так как для определенных уязвимостей (типов уязвимостей) интенсивность их возникновения, как следует из существующей статистики, может быть достаточно велика.

Построение корректных марковских моделей угрозы атаки

Сформулируем и докажем несколько важных утверждений, касающихся рассмотренной проблемы моделирования угрозы атаки.

Аксиома. Марковская модель с дискретными состояниями и непрерывным временем при стационарных потоках входных случайных событий корректна при условии корректного вероятностного разрежения ею всех входных потоков случайных событий.

Утверждение 1. Модель угрозы атаки, как системы без потерь с дискретными состояниями и непрерывным временем, корректна в общем случае (без соответствующих допущений) только при условии, что из каждого состояния на графе системы состояний случайного процесса исходят все I входных потоков событий с интенсивностями λ_i, $i = 1, ..., I$.

Доказательство. Только при выполнении этого условия в общем случае (без каких-либо допущений) для всех I входных потоков событий с интенсивностями λ_i, $i = 1, ..., I$, будет выполняться условие $\lambda_п = \lambda_i$, что подтверждает корректность вероятностного разрежения входных потоков случайных событий для этой модели и, в том числе, обусловливает корректность определения на такой модели надежностных параметров и характеристик безопасности угрозы атаки.

Утверждение 2. В общем случае (без каких-либо обоснованных допущений) для моделирования угрозы атаки должны использоваться счетные (с бесконечным числом состояний) марковские модели с дискретными состояниями и непрерывным временем.

Доказательство. Условие того, что из каждого состояния на графе системы состояний случайного процесса исходят все I входных потоков случайных событий с интенсивностями λ_i, $i = 1, ..., I$, выполнимо только при бесконечном числе состояний на графе.

Выводы.

1. Число возможных состояний в марковской модели с дискретными состояниями и непрерывным временем должно быть счетным, поскольку при конечном числе состояний в модели некорректно разрежаются входные потоки.

2. Марковская модель с дискретными состояниями и непрерывным временем без потерь может применяться для математического моделирования объектов, характеризуемых возможностью одновременного (не одномоментного) возникновения в системе двух и более событий одного типа.

3. Марковская модель с дискретными состояниями и непрерывным временем может применяться для математического моделирования угроз атак, поскольку в системе возможно одновременное возникновение нескольких реальных угроз уязвимостей реализации одного типа.

Пример графа переходов корректной модели угрозы атаки для случая возникновения в системе двух типов угроз уязвимостей реализации для случая, ранее проиллюстрированного на рис. 1, *а*, приведен на рис. 4.

Замечание. Аналогичным образом может быть построена модель для любого числа типов угроз уязвимостей.

На графе представлены следующие обозначения состояний системы: S_{ij}, где i — число возникших и не устраненных уязвимостей реализации первого типа, j — число возникших и не устраненных уязвимостей реализации второго типа.

При существовании в системе только одного потока событий представленный на рис. 3 граф вырождается в схему "гибели и размножения" с бесконечной очередью (все выявляемые уязвимости должны устраняться) и с n обслуживающими приборами — каналами обслуживания; предполагаем, что n выявленных в системе уязвимостей (естественно, в данной системе одного типа) могут устраняться одновременно, остальные же будут ожидать в очереди на обслуживание (рис. 5) [11].

Замечание. Все сказанное в полной мере относится и к невосстанавливаемым системам, которые могут использоваться для моделирования угрозы атаки, направленной на нарушение конфиденциальности обрабатываемой информации, поскольку конфиденциальность похищенной информации не восстанавливаема. В данном случае при моделировании используется поглощающее (из которого нет переходов) состояние $S_а$ (рис. 6).

Однако, как ранее отмечали, нам необходима именно конечная (с конечным числом состояний) марковская модель, поскольку, в отличие от теории массового обслуживания, в данном случае моделируются не обслуживающие приборы, а интенсивности переходов между состояниями, для чего используется модель вероятностного разрежения входных потоков случайных событий. Понятно, что любое математическое моделирование предпо-

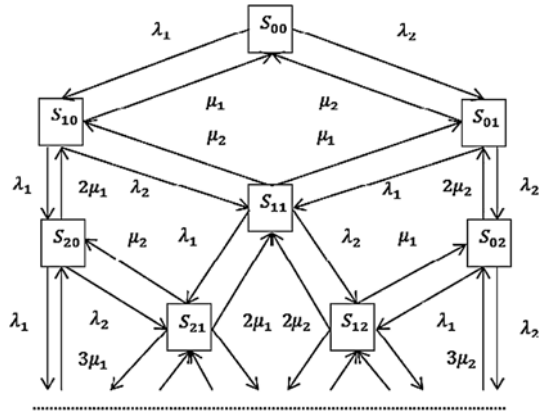

Рис. 4. Размеченный граф системы состояний случайного процесса корректной модели

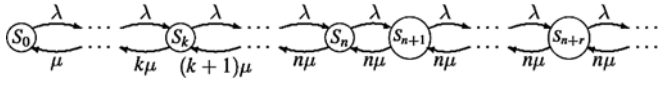

Рис. 5. Схема гибели и размножения

лагает некий набор обоснованно сделанных допущений. Рассмотрим, каким образом можно сделать обоснованные допущения для перехода от корректной счетной к конечной модели угрозы атаки.

В целях обоснованного введения соответствующих допущений для моделирования воспользуемся законом Пуассона (поскольку мы используем простейший — пуассоновский — входной поток при моделировании) [11]. Вероятность того, что на некотором произвольно взятом на временной оси интервале времени t наступит ровно m событий $P_m(t)$, поток которых характеризуется интенсивностью возникновения событий λ, определяется выражением

$$P_m(t) = \frac{(\lambda t)^m}{m!}\mathbf{e}^{-\lambda t}.$$

Нас интересует вероятность возникновения в системе одновременно (не одномоментно) нескольких событий — одновременное выявление нескольких уязвимостей реализации одного типа на интервале времени устранения уязвимостей реализации этого типа, средней продолжительности $t = 1/\mu$. Используя параметр нагрузки (или коэффициента нагрузки) $\rho = \lambda/\mu$, можем определить требуемую нам вероятность

$$P_m(\rho) = \frac{\rho^m}{m!}\mathbf{e}^{-\rho}.$$

Естественно, что на точность моделирования сказывается то, какие состояния S_{ij} в модели (см. рис. 4), мы можем исключить, сделав тем самым исходную счетную модель конечной.

Результаты расчетов $P_m(\rho)$ — вероятности того, что при значении нагрузки $\rho = \lambda/\mu$ за произвольно взятый на временной оси интервал времени $t = 1/\mu$ (продолжительность устранения возникшей реальной угрозы уязвимостей реализации) в информационной системе одновременно будет выявлено и не устранено m уязвимостей реализации этого типа, приведены в таблице.

Как видим из таблицы, необходимость учета вероятностей $P_{m>1}(\rho)$ для угроз уязвимостей реализации при моделировании определяется значением характеристики ρ и требованиями к точности модели. При этом подход к построению корректной модели угрозы безопасности состоит в следующем.

Для каждого типа угрозы уязвимостей, с учетом заданных требований к точности моделирования, посредством расчета значений вероятностей $P_m(\rho)$ определяется число max$i$ учитываемых при моделировании одновременно возникающих в системе уязвимостей одного типа (событий). Все состояния

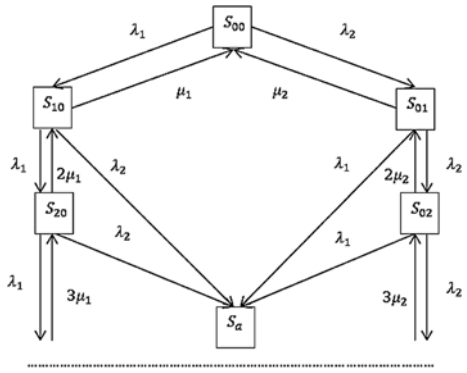

Рис. 6. Размеченный граф системы состояний случайного процесса корректной модели невосстанавливаемой системы

$S_{i>\max ij}$ и дуги между ними исключаются из размеченного графа системы состояний случайного процесса счетной модели, в результате чего получаем искомую корректную (в части вводимых допущений) конечную модель угрозы атаки, корректность которой обосновывается тем, что вероятность события — появление одновременно max$(i + 1)$ уязвимостей одного типа, не сказывается на результатах моделирования с требуемой точностью.

Приведем пример построения корректной конечной модели угрозы атаки. Построим конечную модель угрозы атаки, создаваемой двумя типами угроз уязвимостей реализации (см. рис. 1, *а*) в предположении, что применительно к первой угрозе уязвимостей (первого типа) необходимо учитывать одновременное возникновение в системе двух уязвимостей, для второй же угрозы уязвимостей (второго типа) одновременным появлением в системе нескольких уязвимостей можно пренебречь. В результате вводимых по рассмотренному правилу допущений получим корректную модель угрозы атаки, размеченный граф системы состояний случайного процесса для которой представлен на рис. 7, *а*, модель вероятностного разрежения входных потоков для расчета надежностных параметров угрозы атаки — на рис. 7, *б*.

Оценим корректность данной модели, для чего опять же определим интенсивность первого потока событий, циркулирующего в модели, аналогично тому, как это было сделано для марковской модели, приведенной на рис. 1, *а*. Этот поток событий переводит систему из состояний S_{00}, S_{10}, S_{01}, S_{11} в другие состояния. Как следствие, интенсивность рассматриваемого потока событий в системе $\lambda_{п1}$ определяется уже следующим образом:

$$\lambda_{п1} = (P_{00} + P_{10} + P_{01} + P_{11})\lambda_1.$$

Результаты расчетов

ρ	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
$P_2(\rho)$	0,005	0,016	0,033	0,054	0,076	0,099	0,122	0,144	0,164
$P_3(\rho)$	0	0,001	0,003	0,007	0,013	0,020	0,028	0,038	0,049

В данном случае выполняется условие: $\lambda_{п1} \approx \lambda_1$, за счет введенных допущений при моделировании — из модели исключены состояния, не влияющие на результаты моделирования с требуемой точностью (переходами в которые можно пренебречь).

Универсальность подхода к моделированию угроз атак

Универсальность рассматриваемого подхода к моделированию угроз атак обеспечивается возможностью объединения состояний в модели вероятностного разрежения входных потоков случайных событий, что позволяет формировать состояния, интересующие при проведении соответствующих оценок, и применительно к ним рассчитывать соответствующие параметры и характеристики безопасности. Проиллюстрируем сказанное примером.

Используя построенную модель вероятностного разрежения входных потоков (см. рис. 7, *б*), можем оценить параметры и характеристики безопасности для состояний S_{11} — в системе присутствует одна реальная угроза атаки, и S_{21} — в системе присутствуют одновременно две реальные угрозы атаки:

$$\lambda_{a1} = P_{10}\lambda_2 + P_{01}\lambda_1.$$
$$\lambda_{a2} = P_{20}\lambda_2 + P_{11}\lambda_1.$$

Построим модель для оценки события — в системе присутствует хотя бы одна реальная угроза атаки, т.е. система находится в состоянии отказа безопасности, обозначим это состояние через S_2. Построение соответствующей модели состоит в объединении состояний S_{11} и S_{21} (при этом $P_2 = P_{11} + P_{21}$), в результате чего получаем модель, приведенную на рис. 8.

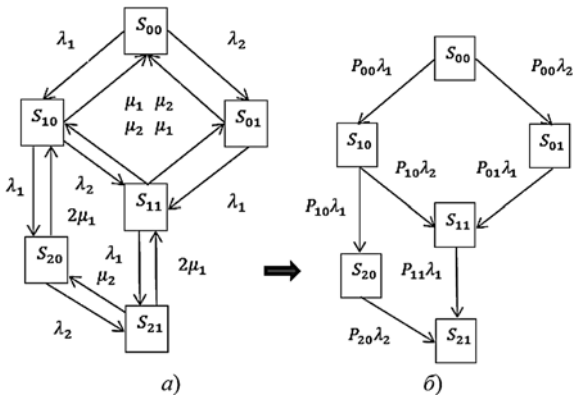

Рис. 7. Иллюстрация преобразования размеченного графа системы состояний случайного процесса корректной марковской модели: *а* — корректная марковская модель угрозы атаки; *б* — модель вероятностного разрежения входных потоков

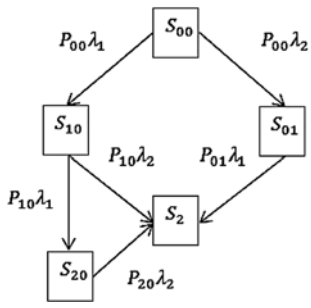

Рис. 8. Модель вероятностного разрежения входных потоков с объединением состояний

Обозначим параметры отказов и восстановлений безопасности информационной системы в отношении угрозы атаки, как λ_0 и $\mu_в$. Для модели, приведенной на рис. 8, они могут быть рассчитаны следующим образом:

$$\lambda_0 = \lambda_2(P_{10} + P_{20}) + P_{01}\lambda_1;$$

$$\mu_в = \frac{(P_{10} + P_{20})\lambda_2 + P_{01}\lambda_1}{P_2} = \frac{(P_{10} + P_{20})\lambda_2 + P_{01}\lambda_1}{P_{11} + P_{21}},$$

где параметр $\mu_в$ рассчитывается с учетом того, что безопасность системы, нарушаемая с интенсивностью λ_0, восстанавливается за долю времени $P_2 = P_{11} + P_{21}$ (это доля времени нахождения системы в объединенном состоянии S_2).

Замечание. Несложно показать, что для λ_0 справедливо соотношение

$$\lambda_0 = \lambda_{a1} + \lambda_{a2} - P_{11}\lambda_1.$$

Соответствующим образом, как это было рассмотрено ранее (с использованием λ_0 и $\mu_в$, по формулам (1) рассчитываются и требуемые характеристики безопасности угрозы атаки.

Сформулируем требование к корректности объединения состояний в модели вероятностного разрежения входных потоков случайных событий.

Утверждение 3. Корректное объединение состояний на графе системы состояний случайного процесса реализуется в том случае, если из объединяемых состояний под воздействием одного и того же потока входных случайных событий реализуются переходы в одно и то же, в том числе объединенное, состояние.

Доказательство. В противном случае невозможно построение корректной марковской модели, поскольку под воздействием одного и того же потока входных случайных событий без какого-либо его разрежения должен осуществляться переход из одного состояния сразу в несколько состояний на графе системы состояний случайного процесса.

Как видим, изложенный подход к моделированию универсален в том смысле, что при его использовании, за счет возможности объединения событий в модели вероятностного разрежения входных потоков, могут моделировать различные события применительно к угрозе атаки, причем, как на информационную систему, так и на систему защиты информации.

Заключение

Исследования в данной работе проводились в части рассмотрения подхода к моделированию надежностных параметров и характеристик безопас-

ности угроз атак. Рассмотренный в работе подход к моделированию мы далее будем использовать и применительно к моделированию эксплуатационных параметров и характеристик безопасности, но при этом уже моделируется не угроза атаки, а реализация возникающей в информационной системе угрозы атаки потенциальным нарушителем, при котором учитывается заинтересованность и готовность потенциального нарушителя к реализации реальной угрозы атаки соответствующей сложности для получения им несанкционированного доступа к информации, характеризуемой определенной ценностью для потенциального нарушителя. В данном случае уже будем строить модели с потерями входных случайных событий. Эти вопросы мы рассмотрим в следующей работе.

Список литературы

1. **Щеглов К. А., Щеглов А. Ю.** Интерпретация и моделирование угрозы атаки на информационную систему. Часть 1. Моделирование угрозы уязвимости и интерпретация угрозы атаки // Информационные технологии. 2015. Т. 21. № 12. С. 930—940.
2. **Щеглов К. А., Щеглов А. Ю.** Интерпретация и моделирование угрозы атаки на информационную систему. Часть 2. Моделирование угрозы атаки // Информационные технологии. 2016. Т. 22. № 1. С. 54—64.
3. **Щеглов К. А., Щеглов А. Ю.** Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. 2014. Вып. 106. № 3. С. 52—65.
4. **Котенко Д. И., Котенко И. В., Саенко И. Б.** Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. 2012. Вып. 3 (22). С. 5—30.
5. **Климов С. М., Сычев М. П., Астрахов А. В.** Противодействие компьютерным атакам. Технологические основы: Электронное учебное издание. М.: МГТУ им. Н. Э. Баумана, 2013. [Электронный ресурс]. URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-techno.htm, свободный (10.02.2016).
6. **Zhang S., Song S.** Novel Attack Graph Posterior Inference Model Based on Bayesian Network // Journal of Information Security, 2011. N. 2. P. 8—27.
7. **Kichkaylo T., Ryutov T., Orosz M. D., Neches R.** Planning to Discover and Counteract Attacks // Informatica (Slovenia), 2010, N. 34 (2). P. 159—168.
8. **Gamal M. M., Hasan D., Hegazy A. F.** A Security Analysis Framework Powered by an Expert System // International Journal of Computer Science and Security. 2011. Vol. 4. P. 505—526.
9. **Щеглов К. А.** Постановка и подходы к решению задачи защиты информации от несанкционированного доступа в общем виде // Вестник компьютерных и информационных технологий. 2016. № 1. С. 32—44.
10. **Алиев Т. И.** Основы моделирования дискретных систем. СПб: Изд. СПбГУ ИТМО, 2009.
11. **Вентцель Е. С.** Исследование операций. Задачи, принципы, методология. М.: Высшая школа, 2007.

K. A. Shcheglov, Graduate Student, **A. Yu. Shcheglov,** Professor, e-mail.ru: info@npp-itb.spb.ru;
St. Petersburg university of ITMO, Russia

Correctness and Versatility Problems of Modeling Attack Threats Reliability Parameters and Characteristics Approach

We did research correctness and universalism problems of suggested attack threat modeling approach which allows to determine reliability parameters and characteristics of attack threat security. This approach is based on building attack threat Markov model (a model with discrete states and continuous time) with its following transformation to input streams probability rarefaction model. Input streams probability rarefaction model based research allowed to do the conclusion that discrete states and continues time Markov model must be counting (not finite) and that such model use is correct for solving attack threats modeling problem. We suggest an approach to elaborate assumptions for counting Markov model transformation into finite model with the usage of Poisson law. We researched universalism problem of suggested attack threat modeling approach basing on states unification possibility in input streams rarefaction probability model.

Keywords: *attack threat, vulnerability threat, reservation, leveling, mathematical modeling, security parameters and characteristics, informational security reliability, attack threat actuality quantitative measure, Markov model, input streams rarefaction*

References

1. **Shcheglov K. A., Shcheglov A. Yu.** Interpretaciya i modelirovanie ugrozy ataki na informacionnuyu sistemu. CHast' 1. Modelirovanie ugrozy uyazvimosti i interpretaciya ugrozy ataki, *Informacionnye tekhnologii*, 2015, vol. 21, no. 12, pp. 930—940 (in Russian).
2. **Shcheglov K. A., Shcheglov A. Yu.** Interpretaciya i modelirovanie ugrozy ataki na informacionnuyu sistemu. Chast' 2. Modelirovanie ugrozy ataki, *Informacionnye tekhnologii*, 2016, vol. 22, no. 1, pp. 54—64 (in Russian).
3. **Shcheglov K. A., Shcheglov A. Yu.** Matematicheskie modeli ehkspluatacionnoj informacionnoj bezopasnosti, *Voprosy zashchity informacii*, 2014, vyp. 106, no. 3, pp. 52—65 (in Russian).
4. **Kotenko D. I., Kotenko I. V., Saenko I. B.** Metody i sredstva modelirovaniya atak v bol'shih komp'yuternyh setyah: sostoyanie problemy, *Trudy SPIIRAN*, 2012, vyp. 3 (22), pp. 5—30 (in Russian).
5. **Klimov S. M., Sychev M. P., Astrahov A. V.** *Protivodejstvie komp'uternym atakam. Tekhnologicheskie osnovy*: EHlektronnoe uchebnoe izdanie, Moscow: MGTU imeni N. EH. Baumana, 2013. [EHlektronnyj resurs]. URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-techno.htm, svobodnyj (10.02.2016) (in Russian).
6. **Zhang S., Song S.** Novel Attack Graph Posterior Inference Model Based on Bayesian Network, *Journal of Information Security*, 2011, no. 2, pp. 8—27.
7. **Kichkaylo T., Ryutov T., Orosz M. D., Neches R.** Planning to Discover and Counteract Attacks, *Informatica* (Slovenia), 2010, no. 34 (2), pp. 159—168.
8. **Gamal M. M., Hasan D., Hegazy A. F.** A Security Analysis Framework Powered by an Expert System, *International Journal of Computer Science and Security*, 2011, vol. 4, pp. 505—526.
9. **Shcheglov K. A.** Postanovka i podhody k resheniyu zadachi zashchity informacii ot nesankcionirovannogo dostupa v obshchem vide, *Vestnik komp'uternyh i informacionnyh tekhnologij*, 2016, no. 1, pp. 32—44 (in Russian).
10. **Aliev T. I.** *Osnovy modelirovaniya diskretnyh sistem*. SPb: Izd. SPbGU ITMO, 2009 (in Russian).
11. **Ventcel' E. S.** *Issledovanie operacij. Zadachi, principy, metodologiya*, Moscow, Vysshaya shkola, 2007 (in Russian).