УДК 004.056.53
DOI: 10.17586/0021-3454-2016-59-12-980-990

МОДЕЛИРОВАНИЕ УГРОЗ АТАК НА ЗАЩИЩЕННУЮ ИНФОРМАЦИОННУЮ СИСТЕМУ

К. А. Щеглов, А. Ю. Щеглов

Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: info@npp-itb.spb.ru

Предложена интерпретация задачи защиты информации как задачи резервирования угроз уязвимостей информационной системы угрозами уязвимостей системы защиты информации. Такой подход позволяет определять и моделировать надежностные параметры и характеристики угроз атак на защищенную информационную систему. Предложен и обоснован подход к моделированию надежностных параметров и характеристик угроз атак, сформулированы требования к построению корректных марковских моделей угроз атак с дискретными состояниями и непрерывным временем.

Ключевые слова: *информационная система, система защиты информации, атака, угроза уязвимостей, угроза атаки, резервирование уязвимостей, моделирование, марковская модель, характеристики угроз атак*

Введение. При моделировании атак необходимо воссоздать последовательность действий потенциального нарушителя — его деструктивных воздействий на информационную систему при осуществлении атаки. Наиболее распространенными, как отмечается в исследовании [1], являются модели атак, основанные на графах (графах атак, байесовских сетях, сетях Петри, а также различных расширениях этих формализмов). При этом под графом атак на информационную систему понимается граф, содержащий все известные траектории (сценарии, пути) реализации нарушителем угроз (целей). Широко применяется моделирование атак с помощью байесовских сетей [2]. Преимущество байесовских графов атак состоит в том, что они представляют собой вероятностные модели, где переходы между вершинами графа определяются соответствующими условными вероятностями, а недостатком является необходимость экспертного (в том числе с использованием различных метрик [3]) задания вероятностей возникновения инцидентов, используемых нарушителем при реализации атаки.

При моделировании систем защиты информации используются марковские цепи [4, 5] либо математический аппарат теории массового обслуживания [6], но также требуется экспертное задание такой характеристики безопасности, как вероятность отражения атаки системой защиты информации.

В работе [7] изложен метод моделирования угрозы атаки марковской моделью с дискретными состояниями и непрерывным временем, основанный на введенной в [8] интерпретации угрозы атаки схемой параллельного резервирования создающих ее угроз уязвимостей. В результате моделирования могут быть рассчитаны надежностные параметры и характеристики угрозы атаки. Искомые параметры названы надежностными, поскольку моделируется не атака как процесс последовательного воздействия нарушителем на информационную систему, а именно угроза атаки как процесс возникновения и устранения в системе отказов информационной безопасности — реальных угроз атак. Как следует из ГОСТ 27.002-89, 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 этого определения и проводя моделирование в рамках предложенной интерпрета-

ции угрозы атаки, можно говорить об определении именно надежностных параметров и характеристик безопасности информационной системы, а в общем случае — о надежности информационной безопасности, под которой понимаем свойство информационной системы сохранять во времени в установленных пределах значения всех характеристик безопасности, определяющих способность системы функционировать в безопасном режиме. В рамках предложенного подхода к моделированию задача защиты информации интерпретируется как задача резервирования угрозами уязвимостей системы защиты угроз уязвимостей защищаемой ею информационной системы. Это обусловливается тем, что для реализации атаки на защищенную информационную систему должны присутствовать не только все уязвимости информационной системы, угрозы безопасности которых создают угрозу атаки, но и все уязвимости системы защиты, что позволяет говорить о схеме параллельного резервирования угроз уязвимостей [7, 8].

Достоинством такого подхода к моделированию угрозы атаки является возможность объективного (с использованием существующей статистики, без экспертных оценок) задания входных параметров модели — интенсивности потоков случайных событий возникновения и устранения в информационной системе угроз уязвимостей [9].

В работах [7, 10] исследовались вопросы построения марковских моделей надежности информационной безопасности — моделей угрозы атаки на информационную систему. В настоящей работе будем исследовать вопросы моделирования надежностных параметров и характеристик угрозы атаки на защищенную информационную систему.

Общий подход к моделированию угрозы атаки [7] состоит в приведении построенной марковской модели угрозы атаки с дискретными состояниями и непрерывным временем к модели вероятностного разреживания входных потоков для расчета требуемых характеристик угрозы атаки. Корректность использования при решении рассматриваемых задач моделирования марковских процессов (используем простейший поток случайных событий возникновения в системе уязвимостей и экспоненциальное распределение времени устранения уязвимостей) обоснована в [9].

Замечание. Поскольку моделируется угроза атаки, не требуется учитывать последовательность использования нарушителем уязвимостей системы.

Пусть угроза атаки создается двумя типами угроз уязвимостей реализации (исключены из рассмотрения угрозы технологических уязвимостей, которые должны нивелироваться средством защиты информации, рассматриваются только уязвимости, создаваемые ошибками реализации программных средств [11]), с соответствующими параметрами — интенсивностью выявления и устранения уязвимостей (аналогичным образом можно построить модель для угрозы атаки любой сложности).

Состояния системы обозначим через S_{ij}, где i и j — уязвимости i-го и j-го типа. Размеченный граф системы состояний случайного (марковского) процесса приведен на рис. 1, *а*.

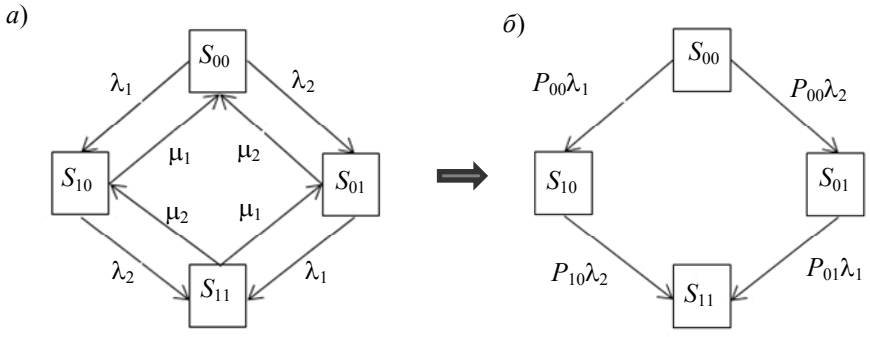

Рис. 1

Поток событий, поступающих на вход марковской модели с интенсивностью λ, вероятностно разреживается — распределяется между состояниями системы S_{ij}, событие может наступить в случайный момент времени, когда система находится в одном из возможных состояний (переходы между состояниями в марковской модели осуществляются мгновенно). Вероятностное разреживание простейшего потока событий приводит к образованию простейших потоков событий (рис. 1, *б*) [12].

При построении этой модели исходим из того, что вероятность P_{ij} 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 [13].

Принципиальное отличие данной модели, приведенной на рис. 1, *б*, от марковской состоит в том, что переходы между состояниями на ней „взвешиваются“ (размечаются) не интенсивностями возникновения случайных событий в системе, а интенсивностями переходов между состояниями. Для обоснования корректности этого преобразования достаточно построить модель вероятностного разреживания потоков (всех потоков, не только входных) в системе.

С использованием модели вероятностного разреживания входных потоков интенсивность возникновения в системе реальной угрозы атаки может быть рассчитана 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 ней реальной угрозы атаки, в каждом из которых система находится с вероятностью $P_{S_{(R-1)}}$, S_R — состояние возникновения в системе реальной угрозы атаки. Переход в состояние S_R из $S_{(R-1)}$ в системе осуществляется с интенсивностью $\lambda_{S_{(R-1)}, S_R}$. Например, для модели, представленной на рис. 1, *б*:

$$\lambda_{\text{a}} = P_{10}\lambda_2 + P_{01}\lambda_1.$$

Поскольку в стационарном режиме функционирования за долю времени нахождения системы в состоянии возникновения реальной угрозы атаки ($1 - P_{0\text{a}}$, где $P_{0\text{a}}$ — вероятность готовности системы к безопасной эксплуатации в отношении угрозы атаки) из состояния, характеризующего реальную угрозу атаки, исходит поступающий в него поток событий λ_{a} (система без потерь, все выявляемые уязвимости устраняются), возможно рассчитать интенсивность устранения с системе реальных угроз атак:

$$\mu_{\text{a}} = \frac{\lambda_{\text{a}}}{1 - P_{0\text{a}}}.$$

Для рассматриваемого примера $\mu_{\text{a}} = \dfrac{P_{10}\lambda_2 + P_{01}\lambda_1}{P_{11}}$

Вероятность готовности информационной системы к безопасной (в отношении угрозы атаки) эксплуатации можно определить как

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

среднее время наработки на отказ безопасности информационной системы (восстанавливаемая система) в отношении угрозы атаки $T_{0\text{уа}}$, среднее время восстановления безопасности информационной системы $T_{\text{вуа}}$ в отношении угрозы атаки:

$$T_{\text{вуа}} = \frac{1}{\mu_{\text{а}}}, T_{0\text{уа}} = \frac{1}{\lambda_{\text{а}}} - T_{\text{вуа}}.$$

Замечание. Согласно рис. 1, *а*, $1/\lambda_{\text{а}}$ — среднее время наработки системы между отказами безопасности $T_{0\text{уа}} + T_{\text{вуа}}$.

Определим корректность использования для моделирования угрозы атаки конечной (с конечным числом состояний [13]) марковской модели с дискретными состояниями и непрерывным временем. Исследовать данную проблему нам позволит модель вероятностного разреживания входных потоков.

Замечание. Если число возможных состояний конечно или счетно (им могут быть присвоены порядковые номера), то случайный процесс называется процессом с дискретными состояниями [13].

Определим интенсивность потока событий, циркулирующего в модели вероятностного разреживания входных потоков, создаваемого возникновением и устранением первой уязвимости. На вход модели для этой угрозы поступает простейший поток событий с интенсивностью λ_1, переводя систему из состояния S_{00}, в котором она находится с вероятностью P_{00}, и из S_{10} с P_{10} (распределяется между двумя состояниями системы S_{00} и S_{10}). Интенсивность потока событий, циркулирующего в модели, определяется следующим образом:

$$\lambda_{n1} = (P_{00} + P_{01})\lambda_1 < \lambda_1.$$

Вызвано это противоречие ($\lambda_{n1} < \lambda_1$) 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 разреживается не между всеми состояниями, т.е. в системе присутствуют интервалы времени, в течение которых события в систему не поступают, что не позволяет говорить о корректности использования в этом случае простейшего (стационарного пуассоновского) входного потока случайных событий. Погрешность моделирования для этого примера тем больше, чем больше $P_{10} + P_{11}$ (в общем случае — это сумма значений вероятностей событий, из которых не выходит анализируемый поток событий).

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

1. Модель угрозы атаки как системы без потерь с дискретными состояниями и непрерывным временем корректна в общем случае, если из каждого состояния на графе системы состояний случайного процесса исходят все I входных потоков событий с интенсивностью λ_i, i=1, …, I.

Доказательство. Только при выполнении этого условия в общем случае для всех I входных потоков событий будет выполняться условие: $\lambda_{ni} = \lambda_i$, что подтверждает корректность вероятностного разреживания входных потоков для этой модели и обусловливает возможность определения на такой модели параметров безопасности угрозы атаки.

2. В общем случае для моделирования угрозы атаки должны использоваться счетные (с бесконечным числом состояний) марковские модели с дискретными состояниями и непрерывным временем.

Доказательство. Условие, что из каждого состояния на графе системы состояний случайного процесса исходят все I входных потоков событий, выполнимо только при бесконечном числе состояний на графе.

Выводы

1. Условием корректности марковской модели с дискретными состояниями и непрерывным временем без потерь является корректное вероятностное распределение входного потока случайных событий между возможными состояниями системы.

2. Такая модель является счетной.

3. Такая модель может применяться для математического моделирования объектов, характеризуемых возможностью одновременного (не одномоментного) возникновения в системе двух и более случайных событий одного типа.

4. Такая модель может применяться для математического моделирования угроз атак, поскольку в системе возможно одновременное возникновение нескольких угроз уязвимостей реализации одного типа [9].

Корректная марковская модель угрозы атаки для рис. 1, *а* представлена на рис. 2.

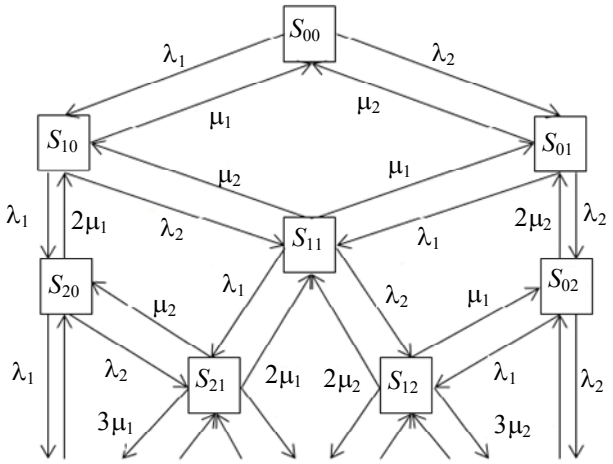

Рис. 2

Поскольку для расчета надежностных параметров и характеристик угрозы атаки необходима модель с конечным числом состояний (моделируются переходы между состояниями системы), определим, каким образом можно перейти к подобной модели посредством введения при моделировании соответствующих допущений.

Поскольку при моделировании используется простейший поток, воспользуемся законом Пуассона [10]. Нас интересует вероятность возникновения в системе одновременно (не одномоментно) нескольких событий — одновременное выявление нескольких уязвимостей одного типа на интервале времени устранения уязвимостей этого типа, средней продолжительности $t=1/\mu$. Используя коэффициент нагрузки $\rho=\lambda/\mu$, определим требуемую вероятность одновременного появления в системе m событий:

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

Точность модели зависит от того, стационарной вероятностью каких состояний пренебрегается. 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. Все состояния $S_{i>\max ij}$ и дуги между ними исключаются из размеченного графа системы состояний случайного процесса счетной модели, в результате чего получается искомая

конечная модель угрозы атаки, корректность (в части вводимых допущений) которой обосновывается тем, что вероятность события — появление одновременно max$i$+1 уязвимостей одного типа — не сказывается на результатах моделирования.

В модель угрозы атаки защищенной информационной системы с использованием в ней системы защиты информации (СЗИ) в горячем резерве включаются угрозы уязвимости СЗИ, выступающие в качестве резервирующих элементов.

Пусть угроза атаки на информационную систему (рис. 3, *б*) создается одной угрозой уязвимостей реализации, применительно к моделированию которой примем допущение о том, что вероятностью появления в системе одновременно более двух типов уязвимостей можно пренебречь, и угроза атаки на СЗИ также создается угрозой уязвимостей одного типа (рис. 3, *а*; вероятностью одновременного появления более одной подобной уязвимости можно пренебречь).

Для таких предположений граф системы состояний случайного процесса для угрозы атаки на защищенную информационную систему приведен на рис. 3, *в*, где i — число выявленных уязвимостей информационной системы, j — число выявленных уязвимостей СЗИ, λ_a и μ_a — параметры безопасности угрозы атаки на информационную систему, $\lambda_{СЗИ}$ и $\mu_{СЗИ}$ — параметры безопасности угрозы атаки на СЗИ.

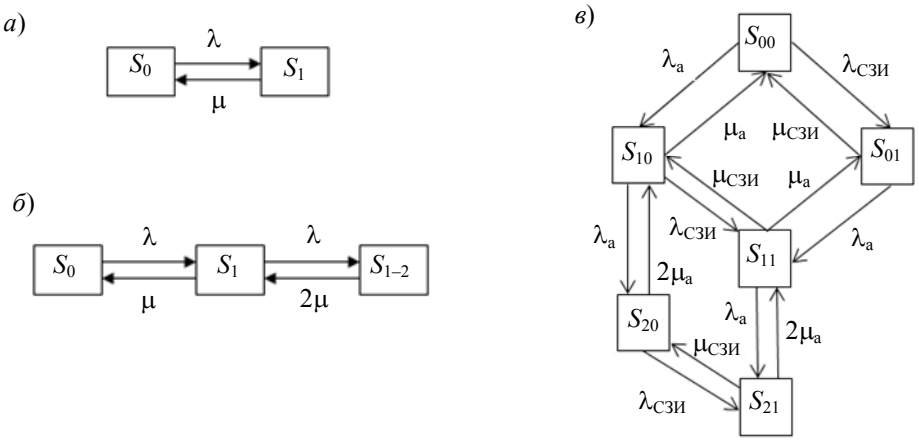

Рис. 3

Используя такую корректную марковскую модель угрозы атаки, можно определить надежностные параметры и характеристики безопасности угрозы атаки на защищенную информационную систему, что предполагает построение модели вероятностного разреживания входных потоков.

Поскольку в системе одновременно могут присутствовать одна (состояние S_{11}) или две реальных угрозы атаки (S_{21}), определим для этих случаев соответственно:

$$\lambda_{a1} = P_{10}\lambda_{СЗИ} + P_{01}\lambda_a,$$
$$\lambda_{a2} = P_{20}\lambda_{СЗИ} + P_{11}\lambda_a.$$

Замечание. Рассчитывая интенсивность λ_{a1}, можно оперировать только входным потоком событий, поскольку именно он определяет возникновение в системе реальных угроз атак вследствие уязвимостей реализации. В частности, при этом не рассматривается поток событий с интенсивностью $P_{21}2\mu_a$, переводящий систему из состояния S_{21} в S_{11} (см. рис. 3), поскольку в этом случае новая уязвимость в системе не возникает, а устраняется одна из возникших в системе уязвимостей.

Соответственно μ_{a1} и μ_{a2} определяются следующим образом:

$$\mu_{a1} = \frac{P_{10}\lambda_{СЗИ} + P_{01}\lambda_a}{P_{11}}, \quad \mu_{a2} = \frac{P_{20}\lambda_{СЗИ} + P_{11}\lambda_a}{P_{21}}.$$

Существенно расширить возможности моделирования можно, объединив состояния в модели вероятностного разреживания входных потоков случайных событий (что позволяет использование при моделировании простейшего входного потока) [10].

Для расчета параметров отказов и восстановлений безопасности в отношении угрозы атаки $\lambda_{\text{о}}$ и $\mu_{\text{в}}$ (где под отказом безопасности будем понимать возникновение в системе хотя бы одной реальной угрозы атаки, под восстановлением безопасности — устранение всех возникших реальных угроз атак) в модели вероятностного разреживания входных потоков требуется объединить все состояния системы, характеризующие наличие хотя бы одной реальной угрозы атаки с сохранением всех исходных переходов в(из) полученное подобным образом состояние. Представленные на рис. 3 состояния S_{11} или S_{21} требуется объединить в состояние S_2 (при этом $P_2 = P_{11} + P_{21}$):

$$\lambda_{\text{о}} = \lambda_{\text{СЗИ}}(P_{10} + P_{20}) + P_{01}\lambda_{\text{а}}.$$

С учетом того, что безопасность системы, нарушаемая с интенсивностью $\lambda_{\text{о}}$, восстанавливается за долю времени $P_2 = P_{11} + P_{21}$, интенсивность восстановления рассчитывается по формуле:

$$\mu_{\text{в}} = \frac{\lambda_{\text{СЗИ}}(P_{10} + P_{20}) + P_{01}\lambda_{\text{а}}}{P_2} = \frac{\lambda_{\text{СЗИ}}(P_{10} + P_{20}) + P_{01}\lambda_{\text{а}}}{P_{11} + P_{21}}.$$

Соответствующим образом рассчитываются надежностные временные характеристики безопасности в отношении угрозы атаки — среднее время между отказами безопасности информационной системы в отношении угрозы атаки $T_{\text{м0о}}$, среднее время наработки на отказ безопасности информационной системы (восстанавливаемая система) в отношении угрозы атаки $T_{0\text{о}}$, среднее время восстановления безопасности информационной системы $T_{0\text{в}}$:

$$T_{\text{м0о}} = \frac{1}{\lambda_{\text{о}}}; \quad T_{0\text{в}} = \frac{1}{\mu_{\text{в}}}; \quad T_{0\text{о}} = T_{\text{м0о}} - T_{0\text{в}}.$$

Вероятность готовности информационной системы к безопасной эксплуатации в отношении угрозы атаки (см. рис. 3) определяется следующим образом:

$$P_{0\text{а}} = P_{00} + P_{10} + P_{01} + P_{20}.$$

Корректное объединение состояний на графе системы состояний случайного процесса происходит, если из объединенных состояний под воздействием одного и того же потока случайных событий реализуются переходы в одно и то же, в том числе объединенное, состояние.

Под холодным резервированием угроз уязвимостей реализации СЗИ будем понимать такой режим ее эксплуатации, при котором угроза условной технологической уязвимости [11] начинает нивелироваться после того, как станет известно о возникновении соответствующей уязвимости, и продолжается до ее устранения.

Использование СЗИ в холодном резерве позволяет снизить нагрузку на вычислительные ресурсы.

Таким образом, холодное резервирование здесь можно рассматривать как некий компромисс между производительностью (влияние СЗИ на загрузку вычислительных ресурсов) и безопасностью информационной системы: защита используется только при реальной угрозе атаки, причем после того, как об ее возникновении становится известно.

В информационной безопасности термин „уязвимость нулевого дня“ обозначает уязвимость, которая известна („опубликована“) и не устранена в системе, как следствие, может использоваться при реализации атаки на информационную систему. Именно „опубликование“ уязвимостей реализации позволяет инициировать процесс нейтрализации создаваемых ими угроз технологических уязвимостей СЗИ.

Существует некий промежуток времени, в течение которого о возникшей в системе уязвимости знает только потенциальный нарушитель: с момента выявления уязвимости до ее „опубликования“.

В течение этого времени при холодном резервировании угроз уязвимостей потенциальный нарушитель может атаковать информационную систему, поскольку еще нет оснований для начала нейтрализации соответствующей угрозы условной технологической уязвимости.

Рассмотрим случаи, когда требуется рассматривать состояние отсутствия резерва (средство защиты еще не включено), т.е. состояние отказа безопасности, и состояние включения резерва — состояние восстановления безопасности. Построим модель холодного резервирования одной угрозы уязвимостей информационной системы одной угрозой уязвимостей СЗИ в предположении, что первая обладает следующими параметрами безопасности: $\lambda_{у}$ — интенсивность возникновения в системе уязвимостей, $\mu_{ув}$ — интенсивность выявления уязвимости — величина, обратная среднему времени между возникновением уязвимости и „опубликованием“ сведений о возникшей уязвимости; $\mu_{уу}$ — интенсивность устранения уязвимости — величина, обратная среднему времени нахождения уязвимости в состоянии „нулевого дня“ (устранения разработчиком уязвимости после „опубликования“ сведений о ней).

Холодное резервирование реализуется СЗИ, также характеризуемой одной угрозой уязвимостей с соответствующими параметрами безопасности $\lambda_{СЗИ}$ и $\mu_{СЗИ}$. Несмотря на то что СЗИ включается только после „опубликования“ сведений, уязвимости собственно в ней могут возникать и устраняться и при отключении СЗИ в информационной системе, поскольку СЗИ может анализироваться потенциальным нарушителем и при выключенном состоянии (в это время она может быть включена в иных информационных системах), т.е. существует вероятность включения СЗИ с возникшей в ней и не устраненной уязвимостью.

Пусть при моделировании введено допущение о том, что вероятностью одновременного появления в системе нескольких уязвимостей информационной системы и СЗИ можно пренебречь.

Размеченный граф системы состояний случайного процесса при холодном резервировании угрозы уязвимостей приведен на рис. 4 (S_{00} — отсутствие в системе не устраненных уязвимостей; S_{10} — отказ безопасности, т.е. возникла, но еще не „опубликована“ резервируемая уязвимость в информационной системе, средство защиты не включено; $S_{10в}$ — „опубликована“ резервируемая уязвимость в информационной системе, начинается ее восстановление разработчиком с интенсивностью $\mu_{уу}$, с целью резервирования включается СЗИ; S_{01} — возникла и не устранена уязвимость в СЗИ; S_{11} — отказ безопасности, т.е. возникли и не устранены уязвимости и в информационной системе, и в СЗИ, но СЗИ еще не выполняет функции резерва, поскольку уязвимость еще не „опубликована“; $S_{11в}$ — отказ безопасности, „опубликована“ резервируемая уязвимость в информационной системе, начинается ее восстановление разработчиком с интенсивностью $\mu_{уу}$, с целью резервирования включается СЗИ, однако в ней не устранена собственная уязвимость).

При построении модели важно, что возникновение уязвимостей в СЗИ не связано с ее состоянием — включена или нет, в частности, это обусловливает наличие перехода из состояния S_{00} в состояние S_{01}.

Таким образом, задача резервирования решается применительно к состояниям системы $S_{10в}$ и $S_{11в}$ (когда уязвимость в информационной системе устраняется разработчиком — состояние „нулевого дня“), отказ безопасности характеризуют состояния S_{10}, S_{11} (уязвимость

информационной системы возникла и отсутствует резерв — СЗИ не включена), и состояние $S_{11в}$ — СЗИ в качестве резервирующего элемента включена, но в ней возникла и не устранена собственная уязвимость.

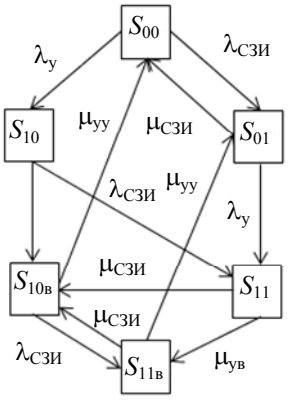

Рис. 4

Вероятность готовности подобным образом резервируемой системы к безопасной эксплуатации $P_{0уСЗИ}$, как следует из рис. 4, может быть определена следующим образом:

$$P_{0уСЗИ} = P_{00} + P_{01} + P_{10в},$$

где $P_{00}, P_{01}, P_{10в}$ — вероятность нахождения системы в состояниях $S_{00}, S_{01}, S_{10в}$.

По аналогии с тем, как это делалось ранее, можно рассчитать значения надежностных параметров и характеристик безопасности угрозы атаки на защищенную информационную систему, но уже при холодном резервировании ее угроз уязвимостей угрозами уязвимостей СЗИ. В частности, для модели, представленной на рис. 4, интенсивность возникновения отказов безопасности в отношении угрозы атаки (объединены состояния $S_{10}, S_{11}, S_{11в}$) $\lambda_о$ может быть рассчитана по формуле:

$$\lambda_о = \lambda_у(P_{00} + P_{01}) + \lambda_{СЗИ}(P_{01} + P_{10в}).$$

Интенсивность восстановлений безопасности в отношении угрозы атаки $\mu_о$ составит

$$\mu_о = \frac{\lambda_у(P_{00} + P_{01}) + \lambda_{СЗИ}(P_{01} + P_{10в})}{P_{10} + P_{11} + P_{11в}}.$$

Соответствующим образом рассчитываются среднее время между отказами безопасности информационной системы в отношении угрозы атаки $T_{м0о}$, среднее время наработки на отказ безопасности информационной системы (восстанавливаемая система) в отношении угрозы атаки $T_{0о}$, среднее время восстановления безопасности информационной системы $T_{0в}$:

$$T_{м0о} = \frac{1}{\lambda_о}; \quad T_{0в} = \frac{1}{\mu_в}; \quad T_{0о} = T_{м0о} - T_{0в}.$$

В заключение отметим, что предложенный подход к моделированию угроз атак на защищенную информационную систему позволяет объективно оценить все необходимые надежностные параметры и характеристики угрозы атаки без использования экспертных оценок, исключительно на основании существующих статистических данных о возникновении и устранении уязвимостей в программных средствах (системных средствах, приложениях, средствах защиты информации), которые непрерывно собираются и публикуются в открытых источниках. Наличие подобных оценок позволяет использовать при проектировании защищенных информационных систем количественные меры актуальности угроз атак, что необходимо для принятия проектных решений по защите информации. Количественная оценка

при моделировании угроз атак на защищенную информационную систему позволяет объективно оценить эффективность средств защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Котенко Д. И., Котенко И. В., Саенко И. Б.* Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Тр. СПИИРАН. 2012. Вып. 3(22). С. 5—30.
2. *Koller D., Friedman N.* Probabilistic Graphical Models. Principles and Techniques. MIT Press, 2009.
3. *Котенко И. В., Степашкин М. В*. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Тр. ИСА РАН. 2007. Т. 31. С. 126—207.
4. *Росенко А. П*. Внутренние угрозы безопасности конфиденциальной информации: Методология и теоретическое исследование. М.: Красанд, 2010.
5. *Иванов К. В., Тутубалин П. И*. Марковские модели защиты автоматизированных систем специального назначения. Казань: ГБУ „Республиканский центр мониторинга качества образования“, 2012.
6. *Карпов В. В*. Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа // Программные продукты и системы. 2003. № 1. С. 31—36.
7. *Щеглов К. А., Щеглов А. Ю.* Марковские модели угрозы безопасности информационной системы // Изв. вузов. Приборостроение. 2015. Т. 58, № 12. С. 957—965.
8. *Щеглов К. А., Щеглов А. Ю*. Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. 2014. Т. 106, № 3. С. 52—65.
9. *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.
10. *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.
11. *Щеглов К. А*. Постановка и подходы к решению задачи защиты информации от несанкционированного доступа в общем виде // Вестн. компьютерных и информационных технологий. 2016. № 1. С. 32—44.
12. *Алиев Т. И.* Основы моделирования дискретных систем. СПб: Изд-во СПбГУ ИТМО, 2009.
13. *Вентцель Е. С*. Исследование операций. М.: Сов. радио, 1972.

Сведения об авторах

Константин Андреевич Щеглов — аспирант; Университет ИТМО; кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Андрей Юрьевич Щеглов — д-р техн. наук, профессор; Университет ИТМО; кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 18.02.16.

Ссылка для цитирования: *Щеглов К. А., Щеглов А. Ю.* Моделирование угроз атак на защищенную информационную систему // Изв. вузов. Приборостроение. 2016. Т. 59, № 12. С. 980—990.

MODELING THREAT OF ATTACK ON A PROTECTED INFORMATION SYSTEM

K. A. Shcheglov, A. Yu. Shcheglov

ITMO University, 197101, St. Petersburg, Russia
E-mail: info@npp-itb.spb.ru

The problem of information security is interpreted as a problem of reservation of threats of information system vulnerabilities by threats of vulnerabilities of the information security system. The approach allows assessing and modeling the threat characteristics and the reliability parameters of protected informa-

tion system. Requirements to development of a valid threat attacks Markov models with discrete states and continuous time are formulated.

Keywords: information system, information security system, attack, threats of vulnerabilities, threat of attack, reservation of vulnerabilities, modeling, Markov models, characteristics of attack threats

Data on authors

Konstantin A. Shcheglov — Post-Graduate Student; ITMO University, Department of Computation Technologies; E-mail: info@npp-itb.spb.ru

Andrey Yu. Shcheglov — Dr. Sci., Professor; ITMO University, Department of Computation Technologies; E-mail: info@npp-itb.spb.ru

For citation: *Shcheglov K. A., Shcheglov A. Yu.* Modeling threat of attack on a protected information system // Izv. vuzov. Priborostroenie. 2016. Vol. 59, N 12. P. 980—990 (in Russian).

DOI: 10.17586/0021-3454-2016-59-12-980-990