УДК 004.056.53

К. А. Щеглов, аспирант, **А. Ю. Щеглов,** д-р техн. наук, профессор,
Исследовательский университет информационных технологий,
механики и оптики, Санкт-Петербург, e-mail: info@npp-itb.spb.ru

Интерпретация и моделирование угрозы атаки на информационную систему. Часть 2. Моделирование угрозы атаки

Построены марковские модели угрозы атаки на информационную систему, как систему с отказами и восстановлениями характеристики безопасности, а также с фатальным отказом, основанные на рассмотрении угрозы уязвимости в качестве простейшего элемента информационной безопасности при интерпретации угрозы атаки схемой последовательного резервирования угроз уязвимостей. Разработана модель нарушителя на основе введенной характеристики сложности реализации угрозы атаки, интерпретируемой, как вероятностная мера количества информации, которой должен обладать нарушитель в отношении угроз уязвимостей, создающих угрозу атаки, для ее реализации. Построенные модели позволяют рассчитывать параметры и характеристики угрозы атаки без необходимости получения каких-либо экспертных оценок, с использованием исключительно стохастических параметров уязвимостей, в отношении которых существует и непрерывно ведется соответствующая статистика.

Ключевые слова: *безопасность, информационная система, угроза атаки, модель, проектирование, потенциальный нарушитель, система защиты информации*

Введение

В работе [1] в качестве простейшего элемента безопасности информационной системы при построении математических моделей угрозы атаки на информационную систему предложено рассматривать угрозу уязвимости, что позволило использовать существующую и непрерывно ведущуюся статистику в отношении выявляемых и устраняемых уязвимостей при задании входных параметров разрабатываемых моделей. Существенным преимуществом предложенного подхода является то, что для задания входных параметров математических моделей не требуется использования каких-либо экспертных оценок, применение которых ставит под сомнение адекватность получаемых результатов моделирования. Кроме того, в работе [1] исследовали вопросы моделирования и оценки актуальности угроз уязвимостей, введена их классификация, разработана модель угрозы уязвимости, как системы с отказами и восстановлениями характеристики безопасности, предложена интерпретация угрозы атаки схемой параллельного резервирования угроз уязвимостей. Определена ключевая задача современных систем защиты информационных систем, состоящая в нивелировании актуальных угроз безусловных и условных технологических уязвимостей. Вместе с тем при проектировании системы защиты информационной системы ключевым элементом моделирования становится угроза атаки, поскольку именно от актуальных угроз атак реализуется защита, посредством нивелирования системой защиты актуальных угроз уязвимостей, создающих угрозу атаки, как следствие, необходимо разработать модели угрозы атаки в целях получения количественной оценки ее актуальности. При моделировании угрозы атаки практический интерес уже представляет не только построение модели с отказами и восстановлениями характеристики безопасности, причем с учетом того, что угроза атаки создается не одной, а в общем случае некоторой совокупностью разнородных угроз уязвимостей, позволяющей получать количественные оценки характеристик возникновения и устранения в системе реальной угрозы атаки, но и построение модели с фатальным отказом, предполагающей уже непосредственно реализацию нарушителем реальной угрозы атаки на конкретную информационную систему (реализацию несанкционированного доступа), для которой проектируется система защиты. С этой целью уже необходимо построить модель нарушителя, позволяющую оценить (опять же без применения экспертных оценок для задания входных параметров для модели нарушителя) готовность реализации атаки

определенной сложности нарушителем на конкретную информационную систему, характеризующую меру его заинтересованности в осуществлении подобной атаки, что в том числе предполагает количественную оценку сложности реализации атаки.

1. Марковские модели угрозы атаки

В работе [1] было дано обоснование корректности использования при моделировании угрозы уязвимости аппарата марковских случайных процессов при допущениях о пуассоновском характере потока заявок и о показательном распределении времени обслуживания и был сделан вывод о том, что при моделировании угрозы безопасности информационной системы, в том числе и при моделировании угроз атак, можно использовать марковские модели, позволяющие определять граничные (худшие) значения характеристик безопасности, которые и необходимы при проектировании систем защиты информационных систем.

1.1. Марковская модель угрозы атаки как системы с отказами и восстановлениями характеристики безопасности. Информационную систему, как в отношении возникновения и устранения угрозы уязвимости, так и в отношении возникновения и устранения угрозы атаки в целом, создаваемой соответствующей совокупностью выявленных уязвимостей, можно рассматривать как систему с отказами и восстановлениями, в нашем случае, характеристики безопасности.

В работах [1, 2] предложено представлять угрозу атаки последовательностью используемых при реализации атаки уязвимостей — орграфом, вершины которого взвешены значениями P_{0yr}, $r = 1, ..., R$, — значениями вероятности отсутствия в системе r-й уязвимости (информационная система готова к безопасной эксплуатации в отношении угрозы r-й уязвимости) — одной из R угроз уязвимостей последовательно (дуги графа определяют последовательность использования выявленных уязвимостей при реализации атаки) используемых атакой на информационную систему (рис. 1).

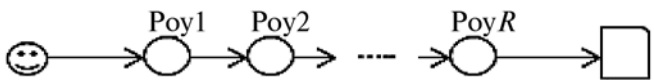

Рис. 1. Орграф угрозы атаки

В работе [1] также предложена классификация угроз уязвимостей, которые подразделены на технологические уязвимости (уязвимости корректности реализации функций защиты) — условные и безусловные, и угрозы уязвимости реализации (в частности, это ошибки программирования системных средств и приложений), возникновение которых в системе позволяет реализовать условные (возникают при условии возникновения соответствующей уязвимости реализации) технологические уязвимости. Поскольку угрозы технологических уязвимостей характеризуются $P_{0yr} = 1$, при построении марковской модели угрозы атаки их вершины необходимо исключать из орграфа угрозы атаки (см. рис. 1), так как модель угрозы атаки строится для приведенного подобным образом орграфа, включающего в себя только размеченные вершины угроз уязвимостей реализации.

Построим марковскую модель, описывающую процесс возникновения и устранения реальной угрозы атаки в информационной системе. Под реальной угрозой атаки понимаем возникновение в системе условий возможности ее реализации нарушителем [1], при которых все уязвимости, угрозы которых создают угрозу атаки (см. рис. 1), выявлены и не устранены.

Отметим, что подобные условия будут, как возникать в системе, что можно интерпретировать, как отказ характеристики безопасности, под которой понимаем свойство системы находиться в безопасном состоянии, так и устраняться, для чего достаточно устранить по крайней мере одну выявленную в системе уязвимость, необходимую для реализации атаки, что можно интерпретировать, как восстановление характеристики безопасности. Таким образом, данной моделью описываются исключительно свойства безопасности системы, собственно реализация атаки на информационную систему нарушителем не моделируется.

Построим марковскую модель и рассмотрим математическое описание марковского процесса с дискретными состояниями и непрерывным временем на примере приведенного орграфа угрозы атаки (см. рис. 1), содержащего (для простоты представления) две взвешенные вершины угроз уязвимостей реализации, — угроза атаки создается двумя уязвимостями, с соответствующими их параметрами — интенсивностями выявления и устранения уязвимостей (аналогичным образом можно построить модель для приведенного орграфа угрозы атаки любой сложности). Граф системы состояний случайного процесса (марковского процесса) приведен на рис. 2, *а*. На графе представлены четыре возможных состояния: S_0 — исходное состояние системы; S_1 — в системе выявлена и не устранена первая уязвимость; S_2 — в системе выявлена и не устранена вторая уязвимость; S_{12} — в системе выявлены и не устранены обе уязвимости — создается реальная угроза атаки. Естественно полагаем, что все переходы системы из одного состояния в другое происходят под воздействием простейших потоков событий с соответствующими интенсивностями выявления или устранения уязвимостей.

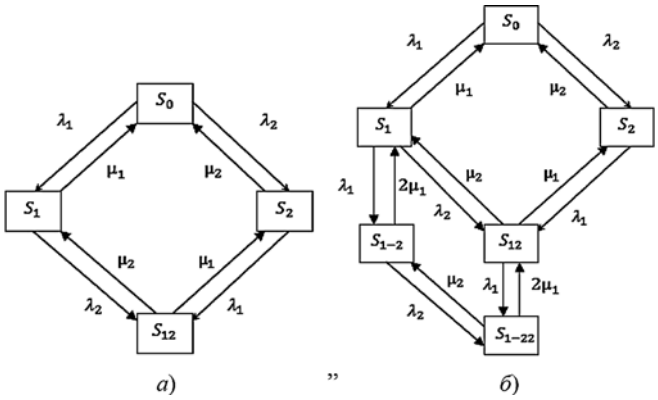

Рис. 2. Графы системы состояний случайного процесса для угрозы атаки:
а — при условии $\rho \leqslant 0{,}2$; *б* — при условии $\rho > 0{,}2$

Система дифференциальных уравнений Колмогорова вероятностей состояний для данного графа будет иметь следующий вид:

$$\begin{cases} P_0' = \mu_1 P_1 + \mu_2 P_2 - (\lambda_1 + \lambda_2) P_0; \\ P_1' = \lambda_1 P_0 + \mu_2 P_3 - (\lambda_2 + \mu_1) P_1; \\ P_2' = \lambda_2 P_0 + \mu_1 P_3 - (\lambda_1 + \mu_2) P_2; \\ P_{12}' = \lambda_2 P_1 + \lambda_1 P_2 - (\mu_1 + \mu_2) P_{12}. \end{cases}$$

Заменяя в уравнениях Колмогорова их производные нулевыми значениями, получим систему линейных алгебраических уравнений, описывающих стационарный режим. Решая эту систему с учетом полной группы событий, т.е., используя условие

$$P_0 + P_1 + P_2 + P_{12} = 1,$$

находим искомые предельные (или финальные) вероятности состояний.

Применительно к рассматриваемой задаче моделирования интерес представляет состояние S_{12} — в системе выявлены обе уязвимости. Характеризуемое вероятностью P_{12} это состояние, в котором создаются условия для осуществления атаки (угроза атаки реальна), т. е. выявлены и не устранены все уязвимости, необходимые для осуществления атаки.

Таким образом, эту характеристику можем далее рассматривать в качестве вероятности возникновения угрозы атаки ($P_{\text{у.а}} = P_{12}$). Соответственно вероятность готовности к безопасной эксплуатации системы в отношении угрозы атаки $P_{0\text{а}}$ (или стационарный коэффициент готовности $K_{\text{г}}$ системы к безопасной эксплуатации) определяется следующим образом:

$$P_{0\text{а}} = K_{\text{г}} = P_0 + P_1 + P_2.$$

Замечание. Для графа, представленного на рис. 2, *а*, $P_{0\text{а}}$ можно рассчитывать по следующей формуле:

$$P_{0\text{а}} = \frac{\mu_1\mu_2 + \lambda_1\mu_2 + \lambda_2\mu_1}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)}. \qquad (1)$$

Модель угрозы атаки (см. рис. 2, *а*) построена в предположении, что для обеих угроз уязвимостей выполняется условие $\rho = \lambda/\mu \leqslant 0{,}2$. В работе [1] проведено соответствующее исследование, в результате которого сделан вывод о том, что при условии $\rho \leqslant 0{,}2$ для моделирования угрозы уязвимости можно использовать одноканальную схему "гибели и размножения" (одновременно можно устранять только одну выявленную в системе уязвимость), при условии же $\rho > 0{,}2$ необходимо использовать двухканальную схему (в системе одновременно можно устранять две выявленные уязвимости).

Включение в модель (см. рис. 2, *а*) двухканальной схемы "гибели и размножения", в предположении, что $\lambda_1/\mu_1 > 0{,}2$, проиллюстрировано на рис. 2, *б*.

Для иллюстрации применения рассмотренных моделей на практике, вновь обратимся к примеру угрозы атаки на повышение привилегий, рассмотренному в работе [1]. Подобная угроза атаки предполагает внедрение на компьютер вредоносной программы, что можно рассматривать как безусловную технологическую уязвимость. Использование выявленной уязвимости реализации (выявленной программной ошибки) в компоненте (программе) ядра ОС, запущенного с системными правами, для исполнения внедренного на компьютер в процессе работы вредоносного файла можно рассматривать уже в качестве условной технологической уязвимости системы (возможно при выявлении соответствующей ошибки в системном средстве), с системными правами. Имеем орграф угрозы атаки, предполагающей последовательное использование нарушителем данных трех уязвимостей (орграф угрозы атаки содержит в своем составе три взвешенных вершины). Интересующий нас приведенный орграф угрозы атаки будет содержать одну взвешенную вершину — вершину соответствующей угрозы уязвимости реализации. Для данной угрозы на основании существующей статистики уязвимостей определяем значения соответствующих параметров безопасности — интенсивность выявления рассматриваемой уязвимости составляет 3 в год, устранения — 12 в год, при этом вероятность готовности к безопасной эксплуатации системы в отношении данной угрозы уязвимости составляет $P_{0\text{у}} = 0{,}75$ [1].

Система защиты включается в орграф угрозы атаки в виде отдельной взвешенной вершины с параметрами безопасности $\lambda_{\text{СЗИ}}$ и $\mu_{\text{СЗИ}}$ уже собственно системы защиты (это параметры угроз уязвимостей системы защиты, куда включены угрозы уязвимости реализации, безусловные и условные угрозы

технологических уязвимостей) [1]. В результате включения вершины системы защиты приведенный орграф угрозы атаки с системой защиты от этой атаки будет содержать две взвешенных вершины.

Замечание. Для упрощения расчетов используем в качестве модели такой системы модель, приведенную на рис. 2, *а* (получим нижнюю — худшую границу характеристики безопасности, так как в данном случае для угрозы уязвимости реализации имеем $\rho = 0{,}25$, что предполагает включение в модель для этой угрозы двухканальной схемы "гибели и размножения" (см. рис. 2, *б*).

Оценим, использовав выражение (1), изменение вероятности готовности к безопасной эксплуатации защищенной информационной системы в отношении угрозы рассматриваемой атаки P_{0a} при изменении параметров безопасности системы защиты $\lambda_{СЗИ}$ и $\mu_{СЗИ}$. Для этого рассмотрим следующие случаи: интенсивность выявления уязвимостей в системе защиты составляет 5 в год при интенсивности их устранения — 20 в год (вероятность готовности к безопасной эксплуатации системы защиты $P_{0уСЗИ} = 0{,}75$), интенсивность выявления уязвимостей в системе защиты — 4 в год при интенсивности их устранения 20 в год ($P_{0уСЗИ} = 0{,}8$), интенсивность выявления уязвимостей в системе защиты — 2 в год при интенсивности их устранения 20 в год ($P_{0уСЗИ} = 0{,}9$), интенсивность выявления уязвимостей в системе защиты — 1 в год при интенсивности их устранения — 20 в год ($P_{0уСЗИ} = 0{,}95$). Результаты расчетов приведены в таблице.

Влияние параметров системы защиты на вероятность готовности информационной системы к безопасной эксплуатации

$P_{0уСЗИ}$	0,75	0,8	0,9	0,95
P_{0a}	0,96	0,97	0,98	0,99

Как видим из таблицы, высокий уровень защищенности информационной системы от актуальной угрозы атаки может быть обеспечен при достаточно невысоких (вполне достижимых на практике) требованиях к значениям параметров безопасности системы защиты.

Отметим, что представленные модели отображают следующее важное свойство угрозы атаки: характеристики угрозы атаки зависят только от набора угроз уязвимостей, создающих угрозу атаки, и их параметров безопасности (набора взвешенных вершин в орграфе атаки) и не зависят от очередности использования выявленных уязвимостей при реализации атаки (не зависят от последовательности переходов между взвешенными вершинами в орграфе атаки). Как следствие, две угрозы атаки, имеющие одинаковый набор взвешенных вершин в орграфе угрозы атаки, эквивалентны — имеют одинаковые характеристики.

Как видим, для расчета значений характеристик угрозы атаки не требуется использования каких-либо экспертных оценок. Адекватность подобной модели угрозы атаки обусловливается использованием объективных значений требуемых для проведения расчетов параметров угроз уязвимостей, получаемых на основании существующей их статистики.

1.2. Укрупненная марковская модель угрозы атаки как системы с отказами и восстановлениями характеристики безопасности. Построение укрупненной модели угрозы атаки необходимо для расчета следующих важнейших характеристик угрозы атаки: интенсивность возникновения λ_a; интенсивность устранения μ_a реальной угрозы атаки; среднее время наработки на отказ (восстанавливаемая система) характеристики безопасности $T_{0уа}$, определяющее средний интервал времени между отказами характеристики безопасности — возникновениями реальной угрозы атаки. Эти важнейшие параметры и характеристику угрозы атаки, необходимые для проектирования системы защиты информационной системы, должны рассчитываться исходя из того, что в качестве простейшего элемента безопасности информационной системы при моделировании рассматривается угроза уязвимости — именно для угроз уязвимости с учетом существующей статистики определяются параметры безопасности [1].

Основой построения укрупненной модели является использование параметра потока отказов. В марковских моделях надежности параметр потока отказов ω определяется (для стационарного участка) следующим образом:

$$\omega = \sum_{i \in Q_+} P_i \sum_{i \in Q_-} \lambda_{ij},$$

где Q_+ — множество состояний работоспособности системы; Q_- — множество состояний отказа системы; λ_{ij} — интенсивность перехода из i-го работоспособного состояния, вероятность нахождения в котором системы — P_i, в j-е неработоспособное состояние [3].

Параметр потока отказов, характеризующий частоту возникновения событий отказа в восстанавливаемых системах, обратно пропорционален среднему времени между отказами $T_{моа}$, в западной литературе используется аббревиатура MTBF (*Mean Time Between Failures*), строгое доказательство этого отношения приведено в теории восстановления:

$$T_{моа} = \frac{1}{\omega} = T_{0у.а} + T_в,$$

где $T_в$ — среднее время восстановления.

Исходя из того, что $K_г = \dfrac{T_{0у.а}}{T_{0у.а} + T_в}$, имеем $T_{0у.а} = \omega K_г$.

Для построения укрупненной модели угрозы атаки вновь обратимся к модели, представленной на рис. 2, *а* (опять же для наглядности рассматриваем простейший пример), и определимся с тем, как формируется поток отказов характеристики безопасности и каким образом определить его эффективность. Как видим, угроза атаки создается в двух случаях: при переходе из состояния S_1, в котором система находится с вероятностью P_1 (в марковской модели вероятность состояния интерпретируется как относительная доля времени нахождения системы в этом состоянии), в состояние S_{12} (это состояние реальной угрозы атаки), переходы осуществляются с интенсивностью λ_2 (с учетом же соответствующей доли времени нахождения в состоянии S_1 — с интенсивностью $P_1\lambda_2$), и при переходе из состояния S_2, в котором система находится с вероятностью P_2, в состояние S_{12}, переходы осуществляются с интенсивностью λ_1 (с учетом же соответствующей доли времени нахождения в состоянии S_2 — с интенсивностью $P_2\lambda_1$). В нашем случае определяемый подобным образом поток отказов может интерпретироваться как поток возникновения реальной угрозы с интенсивностью λ_a:

$$\lambda_a = \omega = P_1\lambda_2 + P_2\lambda_1.$$

В общем случае значение параметра безопасности угрозы атаки λ_a можно рассчитать по следующей формуле:

$$\lambda_a = \omega = \sum_{i \notin S_{R-1},\, i = 1, \ldots, R} P_{S_{R-1}} \lambda_i,$$

где S_{R-1} — множество состояний системы, число которых R, характеризуемых $R-1$ из R возможных (за исключением i-й) выявленных и не устраненных уязвимостей. В каждом из состояний система находится с вероятностью $P_{S_{R-1}}$, из которых осуществляется переход в состояние S_R (все уязвимости выявлены и не устранены — угроза атаки реальна) с интенсивностью λ_i.

Остальные искомые характеристики угрозы атаки рассчитывают по следующим формулам:

$$T_{0y.a} = 1/\lambda_a;$$

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

Отметим, что граф системы состояний случайного процесса укрупненной модели будет иметь два состояния: исходное состояние и состояние, характеризующее выявление и неустранение в системе всех уязвимостей — состояние реальной угрозы атаки с соответствующими интенсивностями переходов между ними λ_a и μ_a.

Приведенные марковские модели можно применять для общей оценки свойств безопасности отдельных средств, в том числе и систем защиты, системных средств, приложений и информационных систем в целом. При проектировании же системы защиты для конкретной информационной системы, используемой для обработки определенной (определенного типа) информации, необходимо учитывать готовность реализации создаваемой в системе реальной угрозы атаки нарушителем, что во многом обусловливается субъективными факторами, определяющими заинтересованность нарушителя в реализации соответствующей атаки на соответствующую информационную систему, используемую для обработки определенной информации. Именно это можно отнести к кардинальным отличиям задачи моделирования в области информационной безопасности от соответствующей задачи моделирования в теории надежности. Таким образом, в разработанные модели необходимо включить состояние фатального отказа, под которым будем понимать успешную реализацию нарушителем атаки на информационную систему. В результате подобного отказа нарушителем осуществляется несанкционированный доступ к информации (например, информация будет похищена), как следствие, в отношении фатального отказа характеристики безопасности система может рассматриваться как невосстанавливаемая.

1.3. Марковские модели угрозы атаки как системы с отказами, восстановлениями и фатальным отказом характеристики безопасности. Состояние фатального отказа в марковской модели угрозы атаки может быть учтено с использованием поглощающей вершины (вершины, не имеющей выхода). Введем понятие коэффициента готовности реализации нарушителем реальной угрозы атаки, обозначим его через $K_{г.а}$, который имеет физический смысл вероятности того, что создаваемая в системе реальная угроза атаки будет реализована нарушителем. Граф системы состояний случайного процесса (марковского процесса), соответствующий системе, граф которой представлен на рис. 2, *а*, но уже с фатальным отказом, представлен на рис. 3.

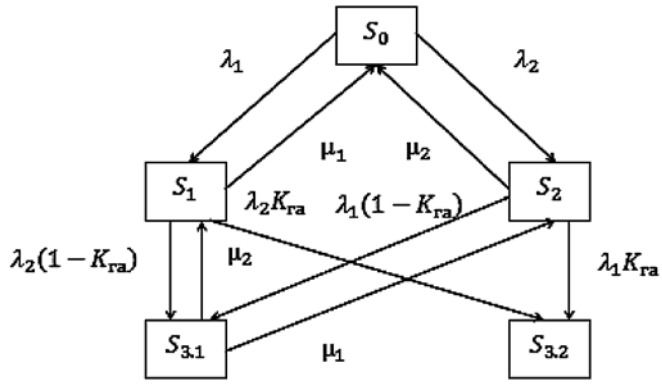

Рис. 3. Граф системы состояний случайного процесса для угрозы атаки с фатальным отказом

При возникновении условия реализации атаки ($P_{\text{у.а}} = 1$, соответственно при вероятности готовности к безопасной эксплуатации $P_{0\text{а}} = 0$) атака будет реализована потенциальным нарушителем с вероятностью $K_{\text{г.а}}$, с вероятностью же $1 - K_{\text{г.а}}$ атаки не произойдет. Это учитывается включением в граф системы состояний случайного процесса, представленного на рис. 2, *а*, вместо вершины S_{12} двух вершин $S_{3.1}$ и $S_{3.2}$ (см. рис. 3). Переход в вершину $S_{3.1}$ предполагает неготовность совершения атаки нарушителем при возникновении ее реальной угрозы (поэтому для этой вершины присутствуют переходы в вершины S_1 и S_2). Переход в вершину $S_{3.2}$ — поглощающую вершину, характеризует реализацию атаки нарушителем на информационную систему.

Как ранее отмечали, значение вероятности P_i состояния (как предельной вероятности) показывает среднее относительное время пребывания системы в *i*-м состоянии. В данном случае эти вероятности рассчитываются так же, как было описано ранее (с учетом того, что из поглощающей вершины нет выхода). Отличие состоит в интерпретации вероятности $P_{\text{у.а}}$ ($P_{\text{у.а}} = P_{3.2}$). В данном случае это вероятность реализации успешной атаки на информационную систему. Для вычисления среднего абсолютного времени пребывания системы в каждом *i*-м состоянии и в системе уравнений Колмогорова нужно положить нулю все производные P_i' ($P_i' = 0$), кроме P_0', если считать, что в начальный момент вероятность первого состояния $P_0 = 1$. Тогда на основании теоремы о дифференцировании изображений в преобразовании Лапласа правая часть первого уравнения будет равна -1. В правых частях уравнений вместо P_i подставляются T_i, и относительно них решается система алгебраических уравнений.

С учетом сказанного, для рассматриваемого примера применительно к графу, приведенному на рис. 3, например, для случая $K_{\text{г.а}} = 1$ (отсутствует вершина $S_{3.1}$, вершину же $S_{3.2}$ обозначим как S_3) получаем

$$\begin{cases} -1 = \mu_1 T_1 + \mu_2 T_2 - (\lambda_1 + \lambda_2) T_0, \\ 0 = \lambda_1 T_0 + \mu_2 T_3 - (\lambda_2 + \mu_1) T_1, \\ 0 = \lambda_2 T_0 + \mu_1 T_3 - (\lambda_1 + \mu_2) T_2, \\ 0 = \lambda_2 T_1 + \lambda_1 T_2 - (\mu_1 + \mu_2) T_3. \end{cases}$$

Рассчитав же значения T_i и просуммировав их для состояний, не являющихся поглощающими, можем вычислить важнейшую характеристику — среднее время наработки системы до отказа характеристики безопасности (система с фатальным отказом — невосстанавливаемая), до реализации на нее успешной атаки — реализации угрозы атаки нарушителем $T_{\text{д0у.а}}$. Например, для системы, описываемой графом, представленным на рис. 3, $T_{\text{д0у.а}}$ определяется следующим образом:

$$T_{\text{д0у.а}} = T_0 + T_1 + T_2 + T_{3.1}.$$

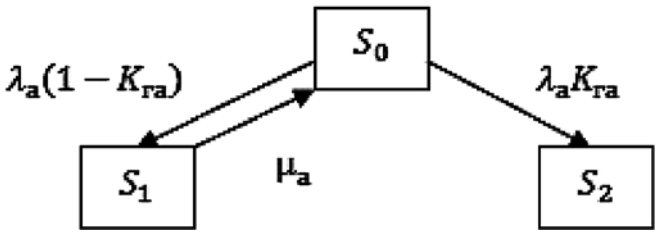

Рис. 4. Граф системы состояний случайного процесса для угрозы атаки с фатальным отказом для укрупненной марковской модели

Граф системы состояний случайного процесса (марковского процесса) укрупненной марковской модели угрозы атаки как системы с отказами, восстановлениями и фатальным отказом характеристики безопасности представлен на рис. 4.

Применение укрупненной марковской модели угрозы атаки как системы с отказами, восстановлениями и фатальным отказом существенно упрощает задачу проектирования системы защиты информационной системы в том случае, когда для используемых в ней средств построены укрупненные марковские модели угрозы атаки как системы с отказами и восстановлениями характеристики безопасности, т.е. определены соответствующие характеристики потенциально возможных для информационной системы угроз атак — интенсивности возникновения $\lambda_{\text{а}}$ и интенсивности устранения $\mu_{\text{а}}$ реальных угроз атак.

Ключевым вопросом возможности и обоснованности практического применения приведенных выше моделей угрозы атаки с фатальным отказом является возможность и обоснованность задания характеристики $K_{\text{г.а}}$ — вероятности (коэффициента готовности) осуществить атаку (реализовать угрозу атаки) потенциальным нарушителем — реализовать создавшуюся в информационной системе реальную угрозу атаки. При этом для возможности использования в модели коэффициент $K_{\text{г.а}}$ необходимо задавать количественно, причем этот коэффициент для возможности моделирования должен быть универсальным для разнородных угроз атак, создаваемых разнородными угрозами уязвимостей. Естественно, что коэффициент $K_{\text{г.а}}$ нужно определять применительно к конкретной информационной системе, обрабатывающей конкретную информацию, которой в конечном счете и определяется заинтересованность и возможность нарушителя в реализации угрозы атаки той или иной сложности на эту систему. Данная задача решается путем построения математической модели потенциального нарушителя безопасности конкретной информационной системы. Опять же для возможности получения адекватных и обоснованных результатов моделирования требованием к построению модели нарушителя является определение значения характеристики $K_{\text{г.а}}$ без использования каких-либо экспертных оценок.

2. Математическая модель потенциального нарушителя

Как отмечали, риск реализации атаки на информационную систему невозможно оценить без построения модели потенциального нарушителя, без подобной модели можно оценить лишь риск отказа безопасности информационной системы. Естественно, что данная модель должна учитывать заинтересованность нарушителя в реализации атаки на конкретную информационную систему и его потенциальные возможности (очевидно, что эти характеристики взаимосвязаны).

В настоящее время модель потенциального нарушителя безопасности формируется как набор предположений о возможном нарушителе безопасности, его квалификации, технических и материальных возможностях и т. д. При этом строится неформальная модель нарушителя, отражающая причины и мотивы действий, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей: способы реализации исходящих от него угроз, место и характер действия, возможная тактика и т. п. В конечном счете подобная модель используется в целях выявления совокупности актуальных угроз атак для конкретной информационной системы, для которой проектируется система защиты информации — именно актуальных, поскольку потенциально возможные угрозы атак на информационную систему определяются возможностью их технической реализации (архитектура, используемые программные и аппаратные средства и т.д.).

Математическое же моделирование нарушителя сводится к моделированию воздействия нарушителя на защищаемую систему и представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, характеризующих результаты действий, и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами защищаемого объекта [4].

Однако подобный подход к моделированию не позволяет количественно оценить актуальность угроз атак, учесть эту важнейшую характеристику безопасности при проектировании системы защиты для конкретной информационной системы.

Для построения математической модели нарушителя в первую очередь введем количественную меру сложности атаки (сложности реализации угрозы атаки), поскольку в общем случае следует говорить о том, готов ли (заинтересован ли и может ли) нарушитель реализовать атаку определенной сложности. При этом необходимо учитывать, что как угрозы уязвимостей, создающие угрозу атаки, так и собственно угрозы атаки по своей сути разнородны, количественная же мера должна быть единой.

Обратимся к основам теории информации, понимая, что для осуществления успешной атаки на отдельно взятую уязвимость, нарушитель должен обладать соответствующей информацией в отношении этой уязвимости — информацией о том, что такая уязвимость выявлена и не устранена, т.е. неким количеством информации в отношении угрозы уязвимости. Так как нас интересует исключительно вероятность того, что уязвимость присутствует в информационной системе, при этом возможны два исхода события: уязвимость присутствует, либо нет. Количество информации в отношении угрозы уязвимости в данном случае следует рассматривать как вероятностную меру.

Замечание. Сложность технической реализации атак на те уязвимости, которые требуют разработки соответствующих программных средств (эксплоитов) для их эксплуатации при реализации атаки, учитывается при задании соответствующего параметра угрозы уязвимости — интенсивности возникновения угрозы уязвимости λ [1]. При задании этого параметра безопасности для угрозы уязвимости на основании анализа соответствующей статистики уязвимостей должна рассматриваться только та часть уязвимостей, для которых за анализируемый период времени подобные эксплоиты были разработаны и использованы [1].

Вероятностная мера количества информации I (в рассматриваемом случае — в одном сообщении) определяется по формуле [5]

$$I = -\log_2 P_i,$$

где P_i — вероятность i-го исхода.

В нашем случае неопределенность можно рассматривать в отношении любой угрозы уязвимости, которую может использовать нарушитель при осуществлении атаки, вероятность ее присутствия (реальная угроза) в системе определяется как $1 - P_{0y}$. Нарушитель для осуществления успешной атаки должен иметь соответствующую информацию, в отношении присутствия уязвимости в системе, т.е. получить сведения, уменьшающие неопределенность в отношении данной угрозы уязвимости. Очевидно, что чем выше для угрозы уязвимости значение P_{0y} (в общем случае уязвимость реже возникает и за меньшее время устраняется), тем сложнее нарушителю осуществить соответствующую атаку.

С учетом сказанного, сложность реализации угрозы уязвимости, обозначим ее S_y, можно интерпретировать как вероятностную меру количества информации $I(P_{0y})$, которой должен обладать злоумышленник для реализации этой угрозы уязвимости, как следствие, может быть определена следующим образом [2]:

$$S_y = I(P_{0y}) = -\log_2(1 - P_{0y}).$$

Корректность применения данной метрики для оценки сложности реализации угрозы уязвимости

обосновывается использованием логарифмической функции (в нашем случае по основанию 2, поскольку у события возможны два исхода), позволяющей соответствующим образом учесть нелинейность функции изменения сложности реализации нарушителем угрозы уязвимости от изменения значения вероятности P_{0y}: $S_y = f(P_{0y})$.

Формулы для расчета характеристики P_{0y} угроз уязвимостей приведены в работе [1].

Проиллюстрируем сказанное примером, для чего сравним сложности реализации двух угроз уязвимостей. Пусть для одной из них значение характеристики P_{0y} составляет 0,7, а для другой — 0,99. Видим, что в первом случае $S_{y1} = 1{,}74$, во втором случае $S_{y2} = 6{,}64$, т.е. реализация угрозы второй уязвимости для нарушителя в 3,82 раза сложнее, чем реализация первой уязвимости (ему понадобится в 3,82 раза больше количества информации об угрозе уязвимости в целях снятия неопределенности в отношении наличия в системе этой уязвимости — создания в системе реальной угрозы) для осуществления успешной атаки на угрозу второй уязвимости, чем на угрозу первой уязвимости.

Замечание. Единица сложности реализации угрозы уязвимости $S_y = I(P_{0y}) = 1$ задается условием $P_{0y} = 0{,}5$, определяющим то, что уязвимость с равной вероятностью присутствует в системе (реальная угроза), либо нет.

Поскольку угрозу атаки создает соответствующая совокупность угроз уязвимостей, сложность атаки для нарушителя в общем случае определяется совокупной сложностью атак на каждую создающую угрозу атаки уязвимость. Если рассмотреть атаку как последовательность использования нарушителем выявленных и не устраненных в системе уязвимостей, имеющих характеристики P_{0yr} и S_{yr}, $r = 1, ..., R$, можно ввести количественную характеристику сложности атаки $I(P_{0a})$, обозначим ее S_a, где $S_a = I(P_{0a})$, определяемую количеством информации, которым должен обладать нарушитель для осуществления успешной атаки, угрозу которой создают R угроз уязвимостей (с учетом того, что события возникновения (выявления) угроз уязвимостей являются независимыми, а условием реализации нарушителем угрозы атаки является наличие в системе одновременно всех уязвимостей, создающих угрозу атаки):

$$S_a = I(P_{0a}) = -\log_2(1 - P_{0a}) = -\log_2 \prod_{r=1}^{R} (1 - P_{0yr}),$$

где $P_{0a} = 1 - \prod_{r=1}^{R} (1 - P_{0yr})$ — вероятность того, что в любой момент времени угроза атаки реальна.

Используя же соответствующее свойство логарифмов, можем записать:

$$S_a = I(P_{0a}) = \sum_{r=1}^{R} I(P_{0yr}) = \sum_{r=1}^{R} S_{yr}.$$

При этом информация в отношении угроз уязвимостей, получаемая нарушителем, рассматривается с точки зрения ее полезности (ценности) для достижения потребителем информации поставленной практической цели, в нашем случае для осуществления злоумышленником успешной атаки на информационную систему.

Замечание. Использование в системе системы защиты, призванной увеличить сложность реализации угрозы атаки, увеличивает значение сложности реализации соответствующей угрозы атаки на информационную систему на значение сложности реализации угрозы атаки на систему защиты информации ΔS_a.

Отметим, что характеристика ΔS_a может рассматриваться в качестве так называемой в теории информации прагматической меры количества информации, определяемой в данном случае по формуле

$$\Delta S_a = \log_2(1 - P_{0a.исх}) - \log_2(1 - P_{0a.защ}) = \log_2 \frac{(1 - P_{0a.исх})}{(1 - P_{0a.защ})},$$

где $P_{0a.исх}$ и $P_{0a.защ}$ — соответственно вероятности готовности к безопасной эксплуатации исходной и защищенной (при использовании системы защиты) информационных систем в отношении угрозы атаки.

Прагматика данной оценки состоит в выявлении условий, при которых необходима реализация соответствующих мер защиты для информационной системы.

Универсальность данной метрики обусловливается тем, что она позволяет сравнивать между собой сложности реализации разнородных атак, основанных на различных принципах реализации, в общем случае использующих совершенно различные угрозы уязвимостей.

Как отмечалось, коэффициент готовности нарушителя осуществить атаку $K_{г.а}$ требуется определять применительно к конкретной информационной системе при проектировании для нее системы защиты. На практике при решении задачи проектирования можно рассматривать (и как правило, рассматривается) некую подобную информационную систему (аналог), характеризуемую обработкой аналогичной информации — именно характеристики обрабатываемой в системе информации определяют заинтересованность и возможности нарушителя. В отношении аналога, как правило, существует соответствующая статистика реализованных (в том числе и отраженных) на информационную систему атак в процессе ее эксплуатации.

С учетом сказанного математическая модель нарушителя (количественная интегральная оценка заинтересованности и возможности реализации нарушителем атаки на конкретную информационную систему) может быть представлена следующим образом:

$$S_{\text{ан}} = \max\{S_{\text{ан}m},\ m = 1,\ ...,\ M\},$$

где $S_{\text{ан}}$ — максимальная сложность реализованных (с учетом и отраженных) в подобной (аналогичной) информационной системе атак, характеризуемых $P_{0\text{ан}}$, определяемая на множестве выявленных совершенных атак на подобную информационную систему (аналог) в процессе ее эксплуатации $S_{\text{ан}m}$, $m = 1,\ ...,\ M$.

Рассчитав же значение характеристики $S_{\text{а}}$ — характеристики сложности реализации атаки на информационную систему, для которой проектируется система защиты, применительно к исследуемой угрозе атаки, и значение характеристики $S_{\text{ан}}$ — характеристики максимальной сложности реализованных (в том числе и отраженных) в подобной информационной системе атак, можно определить искомую характеристику коэффициента готовности нарушителя осуществить атаку сложности $S_{\text{а}}$ (реализовать реальную угрозу атаки, в отношении которой проводится исследование) на конкретную информационную систему (для которой проектируется система защиты) $K_{\text{г.а}}$:

$$K_{\text{г.а}} = \begin{cases} \dfrac{S_{\text{ан}}}{S_{\text{а}}}, \text{ если } S_{\text{ан}} < S_{\text{а}}, \\ 1, \text{ если } S_{\text{ан}} \geqslant S_{\text{а}}. \end{cases}$$

Заметим, что, исходя из того, что

$$K_{\text{г.а}} = \frac{S_{\text{ан}}}{S_{\text{а}}} = \frac{\log_2(1 - P_{0\text{ан}})}{\log_2(1 - P_{0\text{а}})} = \log_{1 - P_{0\text{а}}}(1 - P_{0\text{ан}}),$$

коэффициент $K_{\text{г.а}}$ может интерпретироваться, как значение степени, в которую надо возвести значение вероятности осуществления атаки на информационную систему $(1 - P_{0\text{а}})$, для получения значения вероятности атаки, которую может успешно реализовать нарушитель $(1 - P_{0\text{ан}})$.

Как видим, для расчета значений искомой характеристики $K_{\text{г.а}}$ при применении рассмотренной модели нарушителя не требуется каких-либо экспертных оценок, опять же используются только параметры безопасности угроз уязвимостей и статистика в отношении безопасности эксплуатации аналогичных информационных систем.

3. Моделирование угрозы атаки с использованием аппроксимирующей функции

На практике при проектировании системы защиты при формировании требований к характеристикам безопасности защищаемой информационной системы необходима оценка экономической целесообразности реализации системы защиты той или иной сложности, соответственно, той или иной стоимости, включая стоимость ее эксплуатации. Для этого необходима оценка изменения вероятности фатального отказа характеристики безопасности (соответственно, вероятности готовности к безопасной эксплуатации) в процессе эксплуатации информационной системы [6]. Проиллюстрируем сказанное.

Пусть потери от реализации успешной атаки на информационную систему — несанкционированного доступа к информации (в результате нарушения ее конфиденциальности, целостности или доступности) составляют $C_{\text{инф}}$. Тогда риск потерь применительно к угрозе атаки (характеристика угрозы атаки $P_{0\text{а}}$, соответственно $P_{\text{у.а}} = 1 - P_{0\text{а}}$) можно оценить следующим образом:

$$R_{C_{\text{У.инф}}} = C_{\text{инф}}(1 - P_{0\text{а}}).$$

Если использовать при проектировании системы защиты соответствующую марковскую модель, то определив среднее время наработки информационной системы до реализации на нее успешной атаки (фатальный отказ), определим тем самым средний интервал времени эксплуатации системы, через который потери составят $C_{\text{инф}}$. Данный подход к моделированию не дает возможности ответить на вопрос, а каков будет риск потерь на некотором интервале времени эксплуатации системы, меньшем среднего времени наработки информационной системы до отказа характеристики безопасности, и как риск потерь распределен во времени эксплуатации системы. Важность подобной оценки обусловливается тем, что кроме потенциальных потерь, связанных с несанкционированным доступом к обрабатываемой информации, при внедрении системы защиты присутствуют еще и реальные потери, определяемые стоимостью внедряемой системы защиты $C_{\text{СЗИ}}$ и удельной стоимостью (стоимостью в единицу времени) ее эксплуатации $C_{\text{у.эСЗИ}}(t)$. В первом приближении можно рассматривать линейную зависимость изменения стоимости эксплуатации системы защиты во времени. При этом возникает оптимизационная задача задания требуемого значения характеристики защищаемой информационной системы $P_{0\text{а}}$ при проектировании системы защиты, с учетом того, что потенциальные потери от несанкционированного доступа к обрабатываемой информации при условии $t \to \infty$ стремятся к $C_{\text{инф}}$, в то время как потери, связанные с эксплуатацией системы защиты, при тех же условиях стремятся к ∞ (т.е. задание значения $P_{0\text{а}}$ из условия "чем больше, тем лучше", естественно менее единицы, в общем случае, с учетом сказанного, не корректно).

Задача моделирования состоит в следующем. Как ранее отмечали, в процессе эксплуатации ин-

формационной системы реальная угроза атаки средней продолжительностью $1/\mu_{\text{у.а}}$, в случае, если она не будет реализована нарушителем, в среднем через интервалы времени $T_{0\text{у.а}}$ будет многократно повторяться (характеристика $T_{0\text{у.а}}$ определяется с использованием марковской модели угрозы атаки как системы с отказами и восстановлениями характеристики безопасности). При этом каждую возникающую реальную угрозу атаки злоумышленник может использовать, реализовав атаку с вероятностью $K_{\text{г.а}}$. Иллюстрация сказанного приведена на рис. 5.

Рассчитать значение характеристики $P_{\text{у.а}}$, достигаемое при эксплуатации системы в некоторый момент времени t, кратный $T_{0\text{у.а}}$ при условии $t \geqslant T_{0\text{у.а}}$, обозначив $P_{\text{у.а}}(t \geqslant T_{0\text{у.а}})$, можно следующим образом [6]:

$$P_{\text{у.а}}(t \geqslant T_{0\text{у.а}}) = \sum_{i=1}^{\lceil t/T_{0\text{уа}} \rceil} K_{\text{г.а}}(1 - K_{\text{г.а}})^{i-1},$$

где через $\lceil d \rceil$ обозначено меньшее целое числа d.

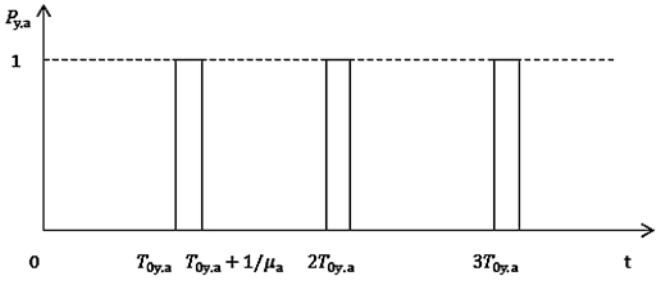

Рис. 5. Иллюстрация появления реальной угрозы атаки в процессе эксплуатации информационной системы

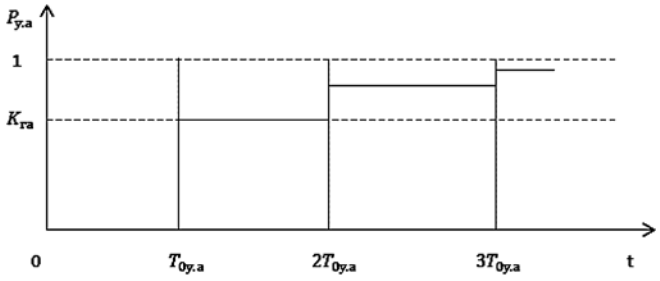

Рис. 6. Иллюстрация изменения характеристики $P_{\text{у.а}}(t \geqslant T_{0\text{у.а}})$ в процессе эксплуатации информационной системы

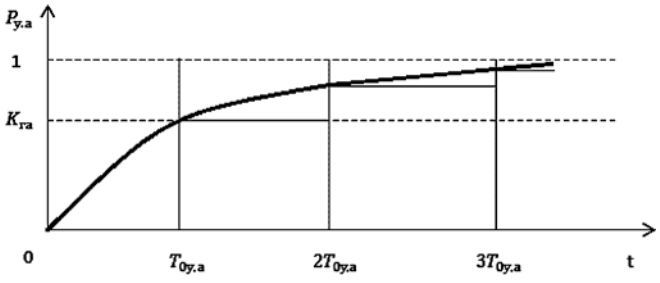

Рис. 7. Иллюстрация аппроксимирующей функции $P_{A\text{у.а}}(t)$

Изменение характеристики $P_{\text{у.а}}$ во времени проиллюстрировано рис. 6.

Для расчета значения $P_{\text{у.а}}(t \geqslant T_{0\text{у.а}})$ в любой момент времени t эксплуатации информационной системы можно построить и использовать соответствующую аппроксимирующую функцию. Основное правило аппроксимации при этом состоит в том, что значение аппроксимирующей функции, обозначим ее $P_{A\text{у.а}}(t)$, для любого момента времени $iT_{0\text{у.а}}$ должно быть не меньше значения функции $P_{\text{у.а}}(t \geqslant T_{0\text{у.а}})$ в соответствующий момент времени — аппроксимирующая функция должна предоставлять возможность получения соответствующей граничной оценки, что требуется при проектировании системы защиты (рис. 7).

Таким образом, с использованием построенной подобным образом аппроксимирующей функции в отношении угрозы атаки можно определить вероятность возникновения реальной угрозы атаки $P_{\text{у.а}}$ на конкретную информационную систему с учетом готовности реализации этой атаки нарушителем в любой момент времени t эксплуатации информационной системы — вероятность фатального отказа, $P_{A\text{у.а}}(t)$, как следствие и значение потенциальных потерь $R_{C_{\text{У.инф}}}(t)$:

$$R_{C_{\text{У.инф}}}(t) = C_{\text{инф}} P_{A\text{у.а}}(t).$$

В общем случае искомая аппроксимирующая функция имеет следующий вид:

$$P_{A\text{у.а}}(t) = (((1/(1 - K_{\text{г.а}}))^{t/T_{0\text{у.а}}} - 1)(1 - K_{\text{г.а}})^{t/T_{0\text{у.а}}}.$$

Заключение

Представленные в работе математические модели позволяют рассчитывать параметры и характеристики угрозы атаки на информационную систему без необходимости получения каких-либо экспертных оценок, с использованием исключительно стохастических параметров безопасности угроз уязвимостей, в том числе и при построении модели потенциального нарушителя. Данные модели можно применять для формирования требований к значениям параметров безопасности системы защиты при ее проектировании для реализации защиты конкретной информационной системы в целях обеспечения требуемого уровня безопасности информационной системы в отношении угрозы атаки. Не рассмотренными в данной работе остались следующие два ключевых вопроса: как оценить угрозу безопасности информационной системы в целом с учетом подверженности ее множеству угроз атак, причем в общем случае зависимых по угрозам уязвимостей, и как оптимальным образом определить те угрозы технологических уязвимостей, которые необходимо нивелировать системой защиты. Эти вопросы авторы предполагают рассмотреть 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. № 12. С. 930—940.
2. **Щеглов К. А., Щеглов А. Ю.** Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. 2014. Вып. 106, № 3. С. 52—65.
3. **Половко А. М., Гуров С. В.** Основы теории надежности. СПб.: БХВ-Петербург, 2006. 704 с.
4. **Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А.** Основы информационной безопасности. М.: Горячая линия — Телеком, 2006.
5. **Шеннон К. Е.** Математическая теория связи. Работы по теории информации и кибернетике: пер. с англ. 1963. С. 243—332.
6. **Щеглов К. А., Щеглов А. Ю.** Эксплуатационные характеристики риска нарушений безопасности информационной системы // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 1 (89). С. 129—139.

K. A. Shcheglov, A. Yu. Shcheglov, Professor,
ITMO University, St. Petersburg, Russian Federation, e-mail: info@npp-itb.spb.ru

Informational System Attack Threat Modeling and Interpretation. Part 2. Attack Threat Modelling

We build Markov's models of attack threat on informational system representing it as a system with failures and recoveries of security characteristics including fatal failures, based on viewing threat as basic element of informational security while interpreting attack threat with a scheme of serial exploit threats reservation. We build the violator model basing on defined attack threat complexity characteristic and interpret it as probabilistic measure of information amount (which must be obtained by violator towards exploit threats creating attack threat). Built models allow to calculate parameters and characteristics of attack threat without need for any experimental estimates with using of exclusively stochastic exploits parameters towards which common statistics exist and being updated.

Keywords: *security, informational system, attack threat, model, design, potential violator, informational security system*

References

1. **Scheglov K. A., Scheglov A. Yu.** Interpretaciya i modelirovanie ugrozy ataki na informacionnuyu sistemu. Chast 1. Modelirovanie ugrozy uyazvimosti i interpretaciya ugrozy ataki, *Informacionnye tehnologii*, 2015, vol. 21, no. 12, pp. 930—940.
2. **Scheglov K. A., Scheglov A. Yu.** Matematicheskie modeli ekspluatacionnoy informacionnoy bezopasnosti, *Voprosy zaschity informacii*, 2014, vol. 106, no. 3, pp. 52—65.
3. **Polovko A. M., Gurov S. V.** *Osnovy teorii nadezhnosti*, SPb.: BHV-Peterburg, 2006, 704 p.
4. **Belov E. B., Los V. P., Mescheryakov R. V., Shelupanov A. A.** *Osnovy informacionnoy bezopasnosti*, Moscow, Goryachaya liniya — Telekom, 2006.
5. **Shennon K. E.** Matematicheskaya teoriya svyazi. *Raboty po teorii informacii i kibernetike*, per. s angl., 1963, pp. 243—332.
6. **Scheglov K. A., Scheglov A. Yu.** Ekspluatacionnye harakteristiki riska narusheniy bezopasnosti informacionnoy sistemy, *Nauchno-tehnicheskiy vestnik informacionnyh tehnologiy, mehaniki i optiki*, 2014, no. 1 (89), pp. 129—139.