УДК 004.056.53
DOI: 10.17586/0021-3454-2016-59-1-50-59

МОДЕЛИРОВАНИЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ АППРОКСИМИРУЮЩИХ ФУНКЦИЙ

К. А. Щеглов, А. Ю. Щеглов

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

Представлен метод моделирования угрозы безопасности информационной системы с использованием аппроксимирующих функций, получаемых с помощью построенной укрупненной марковской модели угрозы атаки. Информационная система рассматривается как система с отказами и восстановлениями характеристики безопасности. Предлагаемый метод позволяет получать принципиально новые и крайне важные для проектирования систем защиты характеристики безопасности информационных систем.

Ключевые слова: *информационная безопасность, угроза атаки, угроза безопасности, моделирование, марковский процесс, аппроксимирующая функция.*

Введение. В работе [1] были предложены интерпретации угрозы атаки на информационную систему и угрозы безопасности информационной системы соответствующими схемами резервирования, а также построена математическая модель нарушителя. В настоящей статье рассматриваются математические модели, позволяющие моделировать важнейшие характеристики угрозы безопасности информационной системы (как системы с отказами и восстановлениями характеристики безопасности) с использованием аппроксимирующих функций, получаемых на основе разработанной укрупненной марковской модели угрозы атаки.

Исходные данные для моделирования угрозы безопасности. В работах [1, 2] угрозы атаки на информационную систему и угрозы ее безопасности предложено представлять соответствующими орграфами. В этом случае угроза атаки может быть представлена схемой параллельного резервирования угроз уязвимостей, а угроза безопасности — схемой последовательного резервирования угроз атак. Обозначим через P_{0an} вероятность того, что информационная система готова к безопасной эксплуатации в отношении n-й угрозы атаки, n=1, ..., N.

Акцентируем внимание на крайне важном моменте моделирования угрозы информационной безопасности. Рассмотрим особенности оценивания вероятности фатального отказа характеристики безопасности. Под отказом характеристики безопасности понимается возникновение в системе одной или нескольких реальных угроз атак (выявлены и не устранены все уязвимости, создающие данную угрозу), а под фатальным отказом понимается осуществление нарушителем успешной атаки (реализация угрозы атаки), т.е. осуществление несанкционированного доступа к обрабатываемой в системе информации. Важным в данном исследовании является то, что сколько бы ни было одновременно создано в информационной системе реальных угроз атак (под реальной понимается угроза, характеризуемая условием $P_{0an} = 0$), которые могут быть реализованы нарушителем, им в любой момент времени будет реализована только одна из угроз, и этого достаточно для нарушения характеристики безопасности (что полностью соответствует представлению угрозы безопасности схемой последовательного резервирования угроз атак [1]). Поскольку в данном случае будет осуществлен несанкционированный доступ к обрабатываемой информации, а это фатальный отказ харак-

теристики безопасности, то далее систему уже не имеет смысла рассматривать как восстанавливаемую — информация похищена. Как следствие, вероятностью реализации нарушителем одновременно двух и более атак можно пренебречь.

Исходя из того, что с вероятностью $1 - P_{0an}$, $n = 1, \ldots, N$, в системе появится n-я реальная угроза атаки, для вероятности перехода системы из безопасного состояния S_0, в котором она находится с вероятностью $P_{0\text{у}}$, в одно из состояний фатального отказа S_n, $n = 1, \ldots, N$ (число состояний системы здесь равно n+1) по причине реализации атаки нарушителем с учетом переходных вероятностей $1 - P_{0an}$ в цепи Маркова можно записать:

$$P_{an} = (1 - P_{0an}) P_{0\text{у}},$$

где P_{an} — вероятность того, что система окажется в n-м состоянии фатального отказа.

Граф переходов цепи Маркова приведен на рис. 1.

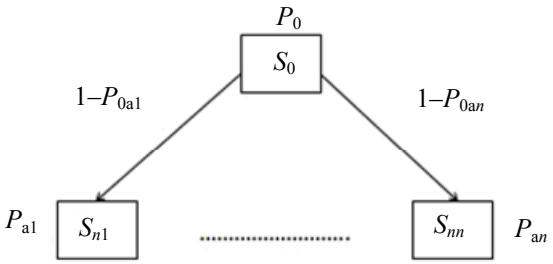

Рис. 1

С учетом же того, что система всегда должна находиться в некотором состоянии

$$P_{0\text{у}} + \sum_{n=1}^{N} P_{an} = 1,$$

получим

$$P_{0\text{у}} = 1 \Big/ \left[1 + \sum_{n=1}^{N} (1 - P_{0an}) \right].$$

Обоснование корректности использования марковских процессов при моделировании угроз атак (при их представлении схемой параллельного резервирования угроз уязвимостей [1]), а также интерпретация результатов, получаемых при подобном подходе к моделированию, как определение граничных (худших) значений характеристики безопасности представлены в работе [3].

Марковские модели угрозы атаки на информационную систему. При рассмотрении информационной системы как системы с отказами и восстановлениями характеристики безопасности реальные угрозы атак будут в системе возникать, но не будут реализовываться нарушителем (т.е. рассматривается система без фатального отказа).

Математическое описание марковского процесса с дискретными состояниями и непрерывным временем рассмотрим на примере орграфа угрозы атаки, содержащего две взвешенные вершины уязвимостей (групп уязвимостей); угроза атаки создается двумя уязвимостями с соответствующими параметрами — интенсивностями выявления и устранения уязвимостей. Граф системы состояний случайного процесса приведен на рис. 2. 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_3 — в системе выявлены и не устранены обе уязвимости. Предположим, что все переходы системы из одного состояния в другое происходят под воздействием простейших потоков

событий с соответствующими интенсивностями выявления (λ) или устранения (μ) уязвимостей, а вероятность одномоментного выявления, равно как и устранения нескольких уязвимостей, пренебрежимо мала.

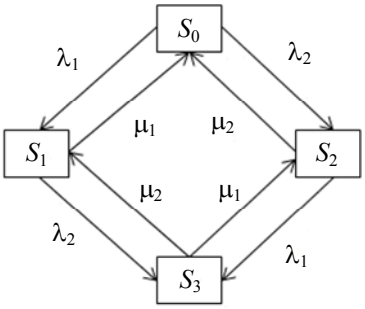

Рис. 2

Для данного графа строится система дифференциальных уравнений Колмогорова и затем соответствующая система линейных алгебраических уравнений, описывающих стационарный режим, решив которую, можно определить вероятности искомых состояний [4]. Применительно к рассматриваемой задаче моделирования интерес представляет состояние S_3, характеризуемое вероятностью P_3, — состояние, в котором выявлены и не устранены все уязвимости, необходимые для осуществления атаки.

Таким образом, эту характеристику можно далее рассматривать в качестве вероятности возникновения угрозы атаки $P_{\text{уа}} = P_3$, соответственно вероятность готовности к безопасной эксплуатации информационной системы в отношении угрозы атаки $P_{0\text{а}} = 1 - P_{\text{уа}}$.

Замечание. Для графа, представленного на рис. 1, значение вероятности $P_{0\text{а}}$ (соответственно и коэффициента готовности к безопасной эксплуатации $K_{\text{г}}$) рассчитывается по следующей формуле:

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

Построение укрупненной модели угрозы атаки необходимо для расчета следующих важнейших характеристик— интенсивности возникновения $\lambda_{\text{а}}$ и интенсивности устранения $\mu_{\text{а}}$ угрозы атаки, а также среднего времени наработки $T_{0\text{уа}}$ на отказ (восстанавливаемая система) характеристики безопасности, определяющего средний интервал времени между отказами характеристики безопасности — возникновениями реальной угрозы атаки. Основу построения укрупненной модели составляет использование параметра потока отказов [5].

В марковских моделях надежности параметр потока отказов ω определяется (для стационарного участка) следующим образом:

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

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

Параметр потока отказов, характеризующий частоту возникновения событий отказа в восстанавливаемых системах, обратно пропорционален среднему времени между отказами

$T_{\text{моа}}$ (в западной литературе используется аббревиатура MTBF — Mean Time Between Failures); строгое доказательство этого отношения приведено в теории восстановления:

$$T_{\text{моа}} = \frac{1}{\omega} = T_{0\text{уа}} + T_{\text{в}},$$

где $T_{\text{в}}$ — среднее время восстановления.

В соответствии с

$$K_{\text{г}} = \frac{T_{0\text{уа}}}{T_{0\text{уа}} + T_{\text{в}}}$$

получим

$$T_{0\text{уа}} = \omega K_{\text{г}}.$$

Для построения укрупненной модели угрозы атаки вновь обратимся к графу, представленному на рис. 2, и выясним, как формируется поток отказов характеристики безопасности и каким образом определить его эффективность. 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_3 (состояние реальной угрозы атаки) переходы осуществляются с интенсивностью λ_2 (с учетом соответствующей доли времени нахождения в состоянии S_1 — с интенсивностью $P_1\lambda_2$);

— при переходе из состояния S_2, в котором система находится с вероятностью P_2, в состояние S_3 переходы осуществляются с интенсивностью λ_1 (с учетом же соответствующей доли времени нахождения в состоянии S_2 — с интенсивностью $P_2\lambda_1$).

В рассматриваемом случае определяемый подобным образом поток отказов может интерпретироваться как поток возникновения реальной угрозы атаки, создаваемый в системе с интенсивностью $\lambda_{\text{а}}$:

$$\lambda_{\text{а}} = \omega = P_1\lambda_2 + P_2\lambda_1.$$

Укрупненная марковская модель угрозы атаки описывается графом, имеющим два состояния: состояние S_0 соответствует отсутствию угрозы, а состояние S_1 — возникновению реальной угрозы атаки, при котором соответствующим образом определяются интенсивности переходов $\lambda_{\text{а}}$ и $\mu_{\text{а}}$. Остальные искомые характеристики угрозы атаки рассчитываются по формулам

$$T_{0\text{уа}} = 1/\lambda_{\text{а}}, \quad \mu_{\text{а}} = \frac{\lambda_{\text{а}} K_{\text{г}}}{1 - K_{\text{г}}} = 1/T_{\text{в}}.$$

Таким образом, в процессе эксплуатации информационной системы реальная угроза атаки продолжительностью $1/\mu_{\text{уа}}$, в случае если она не будет реализовываться нарушителем (система с отказами и восстановлениями), в среднем через интервал времени $T_{0\text{уа}}$ будет многократно возникать, что и проиллюстрировано на рис. 3.

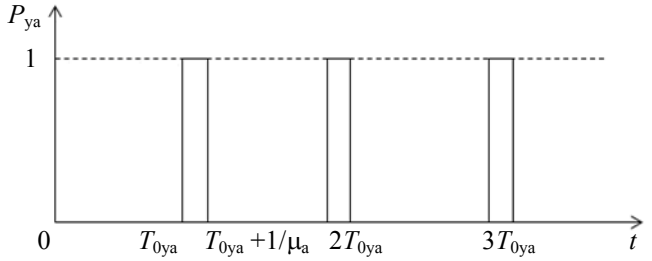

Рис. 3

При проектировании системы защиты информационной системы представляет интерес и моделирование системы с фатальным отказом. При подобном моделировании необходимо учитывать вероятность того, что создаваемая в системе реальная угроза атаки будет реализована нарушителем [6]. В работе [1] построена математическая модель нарушителя, позволяющая определять значение коэффициента вероятности (готовности) реализации злоумышленником угрозы атаки на конкретную информационную систему ($K_{\text{га}n}$). Отметим, что основу данной математической модели составляет представление сложности реализации атаки нарушителем ($S_{\text{a}n}$) как вероятностной меры количества информации, которым должен обладать нарушитель в отношении потенциальной угрозы атаки для ее реализации:

$$S_{\text{a}n} = I\left(P_{0\text{a}n}\right) = -\log_2\left(1 - P_{0\text{a}n}\right).$$

Определив значение характеристики S_{a} — сложности реализации угрозы атаки — и значение характеристики $S_{\text{a max}}$ — максимальной сложности реализованных (в том числе, и отраженных) в аналогичной (либо подобной) информационной системе угроз атак, можно определить искомый коэффициент готовности нарушителя осуществить атаку сложности S_{a} на информационную систему (для которой проектируется система защиты):

$$K_{\text{га}} = \begin{cases} \dfrac{S_{\text{a max}}}{S_{\text{a}}}, \text{ если } S_{\text{a max}} < S_{\text{a}}; \\ 1, \text{ если } S_{\text{a max}} \geq S_{\text{a}}. \end{cases}$$

Имея возможность задать в отношении реальной угрозы атаки коэффициент $K_{\text{га}}$, можно построить соответствующую марковскую модель угрозы атаки на конкретную информационную систему как систему с фатальным отказом. Подобная модель строится посредством включения в исходный граф системы состояний случайного процесса (см. рис. 2) дополнительного „поглощающего“ состояния, соответствующего реализации успешной атаки нарушителем. Так, для графа, представленного на рис. 1, это вершина $S_{3.2}$ на рис. 4 (исходная вершина S_3, см. рис. 2, на рис. 4 обозначена как $S_{3.1}$). Поскольку „поглощающее“ состояние характеризует реализацию успешной атаки (т.е. фатальный отказ характеристики безопасности информационной системы), из него нет выхода. Любой же переход в состояние $S_{3.1}$ в этом случае осуществляется с интенсивностью $(1 - K_{\text{га}})\lambda_i$, а в состояние $S_{3.2}$ — с интенсивностью $K_{\text{га}}\lambda_i$.

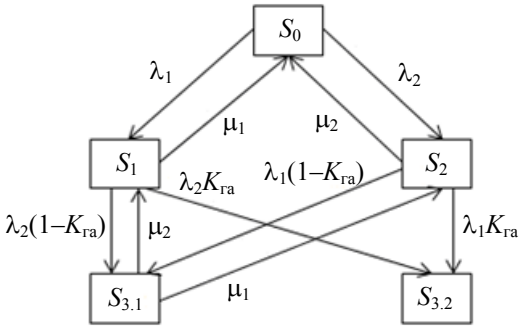

Рис. 4

Рассмотрим, какие характеристики безопасности информационной системы можно определить на подобной модели. Для данного графа строится система дифференциальных уравнений Колмогорова и затем соответствующая система линейных алгебраических уравнений, описывающих стационарный режим, решив которую, можно определить вероятности иско-

мых состояний, в том числе для „поглощающих“ вершин. По аналогии с вышеизложенным можно определить вероятность реализации угрозы атаки на конкретную информационную систему, т.е. вероятность „поглощающего“ состояния. Соответственно вероятность готовности к безопасной эксплуатации конкретной информационной системы в отношении угрозы атаки определяется суммой вероятностей остальных состояний.

Найденные значения вероятностей характеризуют относительное время пребывания системы в соответствующих состояниях. Для вычисления же среднего абсолютного времени пребывания системы в каждом *i*-м состоянии (T_i) в системе уравнений Колмогорова следует принять равными 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 следует подставить T_i и относительно них решить систему алгебраических уравнений. В результате можно определить среднее время наработки системы до отказа характеристики безопасности, так как в данном случае система с отказами характеристики безопасности рассматривается как сумма характеристик T_i состояний, не содержащая характеристики T_i „поглощающего“ состояния.

Таким образом, данная марковская модель позволяет определить две важнейшие характеристики безопасности: вероятность готовности к безопасной эксплуатации конкретной информационной системы в отношении угрозы атаки и среднее время наработки информационной системы до реализации успешной атаки на нее (среднее время наработки до фатального отказа безопасности системы).

Соответствующим образом может быть построена и укрупненная марковская модель с фатальным отказом. Граф системы состояний случайного процесса для укрупненной марковской модели угрозы атаки как системы с отказами, восстановлениями и фатальным отказом характеристики безопасности представлен на рис. 5, где состояние S_0 соответствует отсутствию, а S_1 — возникновению реальной угрозы атаки, состояние же S_2 характеризует фатальный отказ („поглощающее“ состояние).

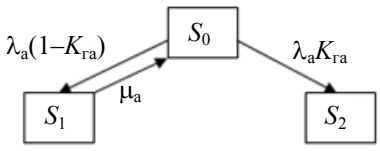

Рис. 5

Моделирование угрозы атаки на информационную систему с использованием аппроксимирующей функции. На практике при решении ключевых задач проектирования системы защиты, в том числе для формирования требований к характеристикам безопасности защищенной информационной системы, включая учет реальных и потенциальных рисков [2], крайне важна оценка изменения значения вероятности отказа характеристики безопасности (соответственно готовности к безопасной эксплуатации) в процессе эксплуатации информационной системы т.е. оценка этой характеристики на некотором интервале времени *t* эксплуатации системы.

Иллюстрация сказанного — изменение характеристики угрозы атаки $P_{уа}\left(t \ge T_{0уа}\right)$ в процессе эксплуатации информационной системы — приведена на рис. 6 [2]. Рассчитать значение $P_{уа}$, достигаемое при эксплуатации системы в некоторый момент времени t, кратный $T_{0уа}$ при условии $t \ge T_{0уа}$, можно следующим образом [2]:

$$P_{\text{уа}}\left(t \ge T_{0\text{уа}}\right) = \sum_{i=1}^{\lceil t/T_{0\text{уа}} \rceil} K_{\text{га}}(1-K_{\text{га}})^{i-1},$$

где $\lceil d \rceil$ — меньшее целое числа d.

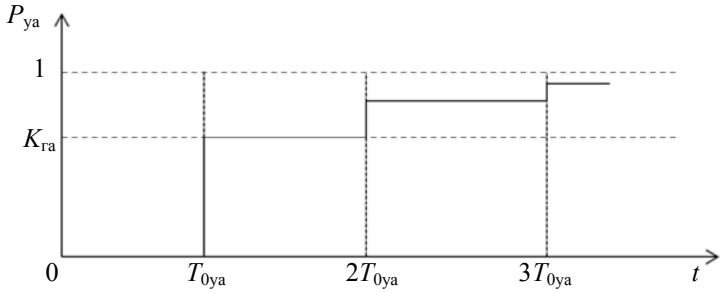

Рис. 6

Для расчета значения $P_{\text{уа}}\left(t \ge T_{0\text{уа}}\right)$ в любой момент времени t необходимо построить соответствующую аппроксимирующую функцию. Основное правило аппроксимации при этом заключается в том, что значение аппроксимирующей функции $P_{\text{Ауа}}(t)$ для любого момента времени $iT_{0\text{уа}}$ должно быть не меньше значения функции $P_{\text{уа}}\left(t \ge T_{0\text{уа}}\right)$ в соответствующий момент времени: аппроксимирующая функция должна обеспечивать возможность получения соответствующей граничной оценки, что требуется при проектировании системы защиты (рис. 7).

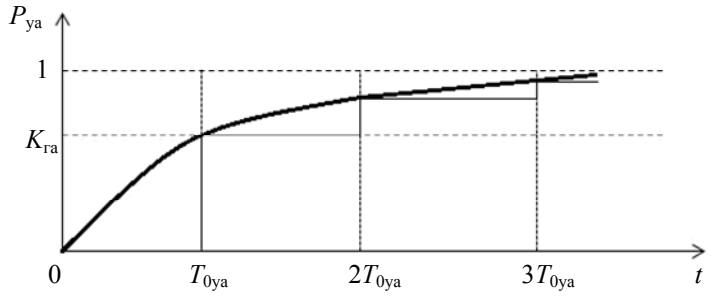

Рис. 7

Таким образом, используя построенную аппроксимирующую функцию в отношении угрозы атаки, можно определить вероятность возникновения реальной угрозы атаки $P_{\text{уа}}$ на конкретную информационную систему с учетом готовности реализации этой атаки нарушителем (соответственно $P_{0\text{а}}=1-P_{\text{уа}}$) в любой момент времени t эксплуатации системы.

В общем случае искомая аппроксимирующая функция имеет следующий вид:

$$P_{\text{Ауа}}(t) = ((1/(1-K_{\text{га}}))^{t/T_{0\text{уа}}} - 1)(1-K_{\text{га}})^{t/T_{0\text{уа}}}.$$

Моделирование угрозы безопасности информационной системы с использованием аппроксимирующих функций. Рассматривая в каждый момент времени t информационную систему как систему с фатальным отказом (с определенной вероятностью) характеристики безопасности (восстановление этой характеристики учтено в аппроксимирующей функции угрозы атаки) и учитывая при этом сделанный ранее вывод о том, что в такой системе не наступит состояния, характеризуемого наличием одновременно двух и более фатальных отказов, при N, n = 1, ..., N, потенциально возможных угрозах атаки, для каждой из которых

может быть построена соответствующая аппроксимирующая функция $P_{\text{Ауа}n}(t)$, вероятность перехода системы из безопасного состояния, в котором она находится в момент времени t с вероятностью $P_{0\text{У}}(t)$, можно описать выражением

$$P_{0\text{У}}(t) = 1 \Big/ \left[1 + \sum_{n=1}^{N} P_{\text{Ауа}n}(t) \right].$$

Вероятность же фатального отказа в момент времени t (на интервале времени t) определяется как $1 - P_{0\text{У}}(t)$.

Отметим, что данный подход к моделированию предполагает использование укрупненной марковской модели угрозы атаки как системы с отказами и восстановлениями характеристики безопасности.

Проиллюстрируем процесс моделирования угрозы безопасности информационной системы с использованием аппроксимирующих функций на примере задачи экономического обоснования принимаемых решений при проектировании системы защиты [2]. Пусть потери от несанкционированного доступа к информации составляют $C_{\text{инф}}$. Тогда риск потерь применительно к угрозе безопасности информационной системы в целом можно оценить следующим образом:

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

Если использовать при проектировании системы защиты соответствующую марковскую модель, то, определив среднее время наработки информационной системы до реализации успешной на нее, т.е. до фатального отказа безопасности системы (в среднем через данный интервал времени характеристика $P_{0\text{У}} = 0$), можно определить средний интервал времени эксплуатации системы, когда потери составят $C_{\text{инф}}$. Данный подход к моделированию не позволяет ответить на вопрос, каков будет риск потерь на некотором интервале времени эксплуатации системы, меньшем среднего времени наработки информационной системы до фатального отказа, 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 ее стоимостью, а также удельной стоимостью (стоимостью в единицу времени) ее эксплуатации. Заметим, что в первом приближении можно рассматривать линейную зависимость изменения стоимости эксплуатации системы защиты во времени. При этом возникает оптимизационная задача задания требуемого значения характеристики $P_{0\text{У}}$ с учетом того, что потенциальные потери от несанкционированного доступа к информации при условии $t \to \infty$ стремятся к $C_{\text{инф}}$, тогда как потери, связанные с эксплуатацией системы защиты при тех же условиях, стремятся к бесконечности (т.е. задание значения $P_{0\text{У}} < 1$ из условия „чем больше, тем лучше“ с учетом сказанного не корректно).

При использовании же аппроксимирующих функций риск потенциальных потерь можно определить как

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

В этом случае риск потенциальных потерь можно оценить для любого момента времени t эксплуатации информационной системы, что позволяет решить рассмотренную оптимизационную

задачу, являющуюся особенно важной при формировании требований к характеристикам безопасности защищенной информационной системы.

Таким образом, предложенный метод моделирования с использованием аппроксимирующих функций характеристики угроз атак позволяет получить принципиально новые и крайне важные для проектирования систем защиты характеристики безопасности информационных систем.

Заключение. Отметим, что результаты, полученные в работе [3] и в данной статье, позволяют в дальнейшем перейти к рассмотрению вопросов проектирования системы защиты информационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. *Щеглов К. А., Щеглов А. Ю.* Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. 2014. Вып. 106, № 3. С. 52—65.
2. *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.
3. *Щеглов К. А., Щеглов А. Ю.* Марковские модели угрозы безопасности информационной системы // Изв. вузов. Приборостроение. 2015. Т. 58, № 12. С. 957—965.
4. *Вентцель Е. С.* Исследование операций. М.: Сов. радио, 1972. 552 с.
5. *Половко А. М., Гуров С. В.* Основы теории надежности. СПб: БХВ-Петербург, 2006. 704 с.
6. *Белов Е. Б., Лось В. П., Мещеряков Р. В., Шелупанов А. А.* Основы информационной безопасности. М.: Горячая линия — Телеком, 2006.

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 06.02.15 г.

Ссылка для цитирования: *Щеглов К. А., Щеглов А. Ю.* Моделирование угрозы безопасности информационной системы с использованием аппроксимирующих функций // Изв. вузов. Приборостроение. 2016. Т. 59, № 1. С. 50—59.

MODELING OF INFORMATION SYSTEM SECURITY THREAT USING APPROXIMATING FUNCTIONS

K. A. Shcheglov, A. Yu. Shcheglov

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

Informational system security threat modeling method is developed using approximating functions designed on the base of pre-built Markov model of attack threat. The information system is considered as a system with failures and restorations of security characteristic function. The proposed method allows deriving principally new and important informational system security characteristics to be used in security system design.

Keywords: informational security, attack threat, security threat, modeling, Markov process, approximating function.

Data on authors

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

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

For citation: *Shcheglov K. A., Shcheglov A. Yu.* Modeling of information system security threat using approximating functions // Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie. 2016. Vol. 59, N 1. P. 50—59 (in Russian).

DOI: 10.17586/0021-3454-2016-59-1-50-59