МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

DOI: 10.24143/2072-9502-2020-2-84-94
УДК 004.942

МОДЕЛЬ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ[1]

И. В. Котенко, И. Б. Паращук

Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург, Российская Федерация

К рассмотрению предлагается разработка математической модели процесса функционирования системы управления информацией и событиями безопасности, известной как SIEM-система. Данная модель представляет собой формализованное аналитическое описание (в терминах марковской цепи в форме разностных стохастических уравнений) динамики смены состояний показателей качества, характеризующих существенные свойства процесса функционирования системы управления информацией и событиями безопасности, в пространстве состояний. Модель представляет собой традиционную для цепи Маркова, в форме конечных разностей, систему уравнений состояния и наблюдения. Научная задача состоит в усовершенствовании (модификации) алгоритмов преобразования шума возбуждения, используемого в модели. Предложен механизм определения значений приращения математического ожидания моделируемого процесса, полученных на основе априорных данных о цепи Маркова, по отношению к математическому ожиданию белого гауссовского шума, возбуждающего этот процесс. Этот механизм позволяет, опираясь на несложные вычисления, принимать решение о том, какие значения будут принимать элементы вектора компенсационных добавок в уравнении состояния вспомогательного вектора индикаторов данной модифицированной модели с учетом преобразования шума возбуждения. Это позволяет упростить модель, снизить ее вычислительную сложность без существенных потерь в точности (адекватности). Практическое применение усовершенствованной модели возможно как в рамках исследовательских работ, так и в системах автоматизированного контроля информационной безопасности.

Ключевые слова: математическое ожидание, система управления информацией и событиями безопасности, показатель качества, процесс функционирования, матрица, состояние.

Для цитирования: *Котенко И. В., Паращук И. Б.* Модель системы управления информацией и событиями безопасности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2020. № 2. С. 84–94. DOI: 10.24143/2072-9502-2020-2-84-94.

Введение

Системы информационной безопасности компьютерных и телекоммуникационных сетей имеют сложную интегрированную структуру. Они включают в себя комплексы аппаратных и программных средств (серверов, баз данных, средств защиты, автоматизированных рабочих мест), а также персонал. Все эти компоненты организационно и технически объединены и предназначены для реализации процесса защиты информации. Цель этого процесса – минимизация потерь, которые могут быть вызваны нарушением доступности, целостности или конфиденциальности информации [1–4].

[1] Работа выполнена при частичной финансовой поддержке РФФИ (проекты 18-07-01488 и 19-07-00953) и бюджетной темы 0073-2019-0002.

Одним из возможных и эффективных подходов к достижению данной цели является разработка и применение систем управления информацией и событиями безопасности (SIEM – Security Information and Event Management). Они предназначены для анализа в реальном времени событий (угроз, тревог) безопасности, исходящих от сетевых устройств и приложений, и позволяют реагировать на эти угрозы до наступления существенного ущерба [5–7].

Актуальность и практическая значимость исследований в рамках данной темы заключаются в формулировке новой модели для описания процесса функционирования SIEM-систем. Это позволит детально аналитически описать работу основного технического решения по обеспечению контроля информационной безопасности (ИБ) – системы управления событиями и инцидентами ИБ, SIEM-системы. Они анализируют информацию, поступающую от различных подсистем ИБ (управления доступом, антивирусной защиты, защиты межсетевого взаимодействия, анализа защищенности, систем обнаружения и предотвращения вторжений, контроля целостности и др.) и выявляют отклонения состояния ИБ по различным критериям. При выявлении отклонения в состоянии ИБ реализуется алгоритм, называемый «управление событиями безопасности» – в подсистеме управления событиями SIEM-системы создается «уведомление», и оповещаются заинтересованные лица. На основе этого оповещения реализуются технические или организационные управленческие решения по предотвращению угроз и противодействию им. Таким образом, SIEM-системы являются инструментом централизованного просмотра и обработки информации, регистрируемой на большом количестве источников за счет графического представления, фильтрации и группировки данных. Выявление отклонений позволяет своевременно и в автоматизированном режиме выявлять угрозы ИБ или предпосылки к их возникновению с учетом совокупности регистрируемых событий и собираемых данных.

Традиционным подходом к аналитическому описанию процессов функционирования сложных систем, например таких, как SIEM-система, являются попытки формально математически представить данные процессы через динамику линейного или нелинейного изменения состояния (пошаговых значений) показателей качества (ПК) SIEM-системы и процесса ее функционирования в пространстве состояний. Марковские модели процессов в этом случае являются незаменимым инструментом.

Под показателями качества SIEM-системы понимается количественная характеристика одного или нескольких свойств этой системы, обуславливающих ее качество. Эта количественная характеристика может иметь векторный вид (вектор ПК), обозначаться как вектор, например, $\vec{x}(k)$. Здесь компоненты вектора ПК $\vec{x}(k)$ представляют собой численные значения одного или нескольких параметров, описывающих конкретное свойство SIEM-системы, а также процессов функционирования различных ее элементов или системы в целом. При этом ПК как количественная характеристика одного или нескольких свойств системы, обуславливающих ее качество, рассматривается применительно к определенным условиям создания SIEM-системы и условиям реализации процесса ее функционирования.

Например, в качестве ПК, характеризующего своевременность выявления SIEM-системой отклонения в состоянии ИБ, может выступать среднее время выявления $\overline{t}_{\text{в}}(k)$ такого отклонения по конкретному критерию (появление вируса, нарушение прав доступа и т. д.). При этом под своевременностью выявления отклонения в состоянии ИБ понимается свойство SIEM-системы, характеризующее ее способность обеспечивать идентификацию отклонения и оповещение о нем в установленные сроки или в реальном масштабе времени.

В состав вектора ПК, характеризующего надежность SIEM-системы, например, могут быть включены параметры: среднее время наработки SIEM-системы на отказ $\overline{t}_{\text{но}}(k)$, среднее время восстановления SIEM-системы $\overline{t}_{\text{вос}}(k)$, коэффициент готовности SIEM-системы $K_{\text{гот}}(k)$ и коэффициент технического использования $K_{\text{ти}}(k)$ SIEM-системы. При этом под надежностью SIEM-системы подразумевается ее способность сохранять в установленных пределах времени значения всех ключевых параметров, определяющих выполнение ею требуемых функций.

Состояние ПК – понятие, обозначающее множество устойчивых значений этого показателя. Их может быть несколько либо большое множество. Состояние ПК характеризуется тем, что описывает переменные свойства этого показателя. При этом состояние какого-либо показателя качества процесса устойчиво до тех пор, пока процесс не реализуется, ведь сам процесс – это

последовательная смена состояний показателей, его описывающих. Математическим языком описания процесса функционирования SIEM-системы как объекта исследования, на наш взгляд, может выступать язык теории множеств и функциональных пространств. В нашей статье рассмотрен подход к описанию математической модели процесса функционирования SIEM-системы как к формализованному описанию процесса смены состояний ПК (движения ПК) в пространстве состояний, причем данное движение является функцией времени. При этом предполагается, что аналитическая, вероятностно-временная модель смены состояний ПК процесса функционирования SIEM-системы может быть построена на основе марковских последовательностей.

В нашем случае в качестве примера могут быть рассмотрены три состояния ПК – три устойчивых значения *j*-го ПК функционирования SIEM-системы. Три состояния ПК – «отлично» (значения ПК удовлетворяют требованиям), «удовлетворительно» (значения ПК «на грани») и «плохо (авария)» (значения ПК не удовлетворяют требованиям).

Необходимыми базовыми исходными данными для аналитического описания процесса функционирования SIEM-системы в данной постановке являются вектор показателей качества (ВПК) SIEM-системы и требования к этим ПК. Тогда модель процесса функционирования SIEM-системы можно представить через аналитическое описание процесса смены состояний (значений) ее ВПК. При этом аналитическое описание ВПК процесса функционирования SIEM-системы, обозначим его $x(k)$, аналитическая взаимосвязь отдельных ПК системы в общем случае динамического, вероятностного, нелинейного и нестационарного процесса ее функционирования связаны с необходимостью задания многомерных функций $F(x, \vec{\lambda}, t_0, \ldots, t_k, \ldots, t_K)$ либо плотностей $W(x, \vec{\lambda}, t_0, \ldots, t_k, \ldots, t_K)$ распределения вероятностей значений параметров (показателей) процессов функционирования различных элементов SIEM-системы и процесса ее работы в целом на интервале функционирования этой системы (t_0–t_K). Математическое описание, с учетом расширения размерности (m – число переменных состояния процесса $x(k)$; s – число параметров распределений; λ и k – количество отсчетов времени), в этом случае затруднительно.

Анализ релевантных работ

Анализ подобных ограничений приводит к необходимости поиска достаточно строгого аналитического описания процесса функционирования SIEM-системы в динамике. На наш взгляд, наиболее корректно данные ограничения могут быть учтены в рамках марковских моделей, рассматриваемых в ряде современных работ.

Работа [8] рассматривает математическое моделирование, основанное на общей теории систем. Здесь предложена модель в абстрактных терминах, что не позволяет полноценно использовать ее для моделирования конкретных угроз в рамках работы SIEM-системы.

В работах [9, 10] утверждается, что модель сложного управляемого процесса может быть реализована на основе стохастических дифференциальных уравнений. Но эти модели требуют значительных затрат на сбор статистики исходных данных для моделирования динамики изменений значений параметров и показателей качества SIEM-систем. Они не обеспечивают потребности пользователя по унификации и удобству (простоте) использования. Эти модели сложны с точки зрения описания динамики процессов. Так, в работах [11–13] предложены приложения моделей, построенных на стохастических дифференциальных уравнениях, но использованные в них традиционные методы определения параметров динамики изменений значений показателей качества объекта моделирования малоэффективны в силу необходимости рассмотрения множества вспомогательных параметров для полноценного описания всех свойств SIEM-систем, а это не всегда возможно.

Работы [14–19] посвящены возможностям математического описания процессов в динамике с использованием марковских цепей. Такие подходы будут рассмотрены и в нашей работе, это будут динамические модели процесса функционирования SIEM-систем. Они являются базой для моделирования, однако эти работы не рассматривают проблему расчета совместной плотности распределения вероятностей различных показателей качества процесса функционирования SIEM-систем. Частично свободна от этих недостатков модель, рассматриваемая в работе [20], однако, хотя она и опирается на цепи Маркова в форме разностных стохастических уравнений, но ориентирована на моделирование процессов обнаружения вредоносной информации. Наиболее близкой по сущности к идее, предлагаемой в данной статье, является работа [21], где предложена марковская модель процесса принятия решений по управлению информацией и событиями безопасности.

Таким образом, из анализа релевантных работ следует, что марковские модели процессов обладают высокой универсальностью, а сочетание теории марковских процессов с теорией переменных состояния открывает широкие возможности для исследования сложных систем, таких как SIEM-система. Иными словами, можно предположить теоретическую и практическую возможность построения аналитических, вероятностно-временных моделей смены состояний процесса функционирования SIEM-системы (как математических моделей смены состояний ПК этих систем) на основе марковских последовательностей, добиваясь требуемой степени адекватности вероятностно-временных свойств процесса функционирования систем такого класса при сокращении размерности их математического описания.

Теоретическая часть

Для построения аналитической вероятностно-временной модели смены состояний ВПК SIEM-системы, учитывающей динамический и вероятностный характер, нестационарность процесса ее функционирования и управления ею, воспользуемся аппаратом управляемых цепей Маркова (УЦМ), описываемых в форме разностных стохастических уравнений (РСУ). Анализ работ [8–21] позволяет говорить, что все известные классы марковских случайных процессов могут быть сведены к эквивалентным им (с точностью до допустимой ошибки моделирования по времени $\Delta t_{\text{доп}}$ и по состоянию $\Delta x_{\text{доп}}$) цепям Маркова. Этот вид модели отличается от используемых ранее, поскольку пока не исследовались возможности применения УЦМ в форме РСУ (УЦМ-РСУ) для векторного анализа качества процесса функционирования SIEM-систем. С учетом результатов анализа можно утверждать, что от стохастических дифференциальных уравнений для разрывных процессов нетрудно перейти к РСУ, которые для дискретных моделей смены состояний ПК процесса функционирования SIEM-системы в форме УЦМ (T = const) будут иметь вид

$$\vec{x}(k+1) = \mathrm{C}^{\mathrm{т}}(k+1)\,\vec{\Theta}(k+1); \tag{1}$$

$$\vec{\Theta}(k+1) = \varphi^{\mathrm{т}}(k+1,\, k,\, u)\,\vec{\Theta}(k) + \vec{\vartheta}(k); \tag{2}$$

$$\vec{\vartheta}(k) = [\vartheta^{\mathrm{т}}(k)\vec{\Theta}(k)]\,\vec{\vartheta}'(k+1); \tag{3}$$

$$\vec{Z}(k+1) = \mathrm{H}(k, x(k))\,\vec{\Theta}(k+1) + \vec{\omega}(k+1), \tag{4}$$

где выражение (1) – уравнение состояния процесса x на $(k + 1)$-м шаге (в нашем случае это состояние некоторого ПК процесса функционирования SIEM-системы), в котором $\mathrm{C}^{\mathrm{т}}(k+1)$ – матрица-строка возможных значений отклонений ПК процесса функционирования SIEM-системы; $\vec{\Theta}(k+1)$ – вспомогательный вектор индикаторов состояния ПК процесса функционирования SIEM-системы, принимающий значения 0 или 1 и вводимый для удобства записи динамики переходов процесса функционирования системы такого класса из состояния в состояние ($m = \overline{1, M}$ – число состояний).

Выражение (2) – уравнение состояния вспомогательного вектора индикаторов, в котором $\varphi^{\mathrm{т}}(k+1, k, u)$ – матрица вероятностей перехода процесса, обуславливающего смену состояний ПК процесса функционирования SIEM-системы; $\vec{\Theta}(k)$ – вектор значений индикаторов состояния на предыдущем шаге; $\vec{\vartheta}(k)$ – вектор компенсационных добавок, элементы которого предназначены для компенсации нецелочисленной части уравнения и получены в результате коррекции исходного шума возбуждения – белого гауссовского шума (БГШ) с математическим ожиданием и дисперсией, соответствующими начальному состоянию оцениваемого ПК процесса функционирования SIEM-системы $\vartheta^{\text{бгш}}(k)$ – уравнение (3).

Справедливость применения в роли шума возбуждения БГШ с адекватными реальному процессу параметрами обусловлена природой случайных значений ПК SIEM-системы; $\vartheta^{\mathrm{т}}(k)$ – диагональная блочная матрица компенсационных добавок, являющаяся ступенчатым мартингалом, элементы которого предназначены для компенсации нецелочисленной части в уравнении (2);

$\vec{\vartheta}'(k+1)$ – вектор значений модифицированного возбуждающего шума, определяющий значения $\vec{\Theta}$ на $(k+1)$-м шаге (значения вспомогательных индикаторов процесса $x\,(k+1)$).

Выражение (4) – уравнение наблюдения за процессом смены состояний ПК процесса функционирования SIEM-системы, где $\vec{Z}(k+1)$ – вектор значений наблюдаемого ПК, $\mathrm{H}(k, x(k))$ – матрица наблюдения, содержащая известные значения наблюдения за состоянием процесса $x(k)$:

$$\mathrm{H}(k, x(k)) = \begin{vmatrix} x_1(k) & 0 & \cdots & 0 \\ 0 & {}_{x_1}(k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x_1(k) \end{vmatrix}; \tag{5}$$

$\vec{\omega}(k+1)$ – вектор шумов наблюдения за процессом смены состояний ПК SIEM-системы $x(k)$ с нулевым средним и матрицей дисперсий $\vartheta_{\omega}(k)$.

Аналитическая модель процесса смены состояний конкретного ПК, например среднего времени $\overline{t}_{\text{в}}(k)$ выявления отклонения в состоянии ИБ, характеризующего своевременность (оперативность) выявления SIEM-системой отклонения в состоянии ИБ, имеет вид

$$\vec{t}_{\text{в}}(k+1) = \mathrm{C}^{\text{т}}_{\overline{t}_{\text{в}}}(k+1)\,\vec{\Theta}_{\overline{t}_{\text{в}}}(k+1); \tag{6}$$

$$\vec{\Theta}_{\overline{t}_{\text{в}}}(k+1) = \varphi^{\text{т}}_{\overline{t}_{\text{в}}}(k+1, k, u)\,\vec{\Theta}_{\overline{t}_{\text{в}}}(k) + \vec{\vartheta}_{\overline{t}_{\text{в}}}(k); \tag{7}$$

$$\vec{\vartheta}_{\overline{t}_{\text{в}}}(k) = [\vartheta^{\text{т}}_{\overline{t}_{\text{в}}}(k)\vec{\Theta}_{\overline{t}_{\text{в}}}(k)]\,\vec{\vartheta}^{/}_{\overline{t}_{\text{в}}}(k+1); \tag{8}$$

$$\vec{Z}_{\overline{t}_{\text{в}}}(k+1) = \mathrm{H}_{\overline{t}_{\text{в}}}(k, x(k))\,\vec{\Theta}_{\overline{t}_{\text{в}}}(k+1) + \vec{\omega}_{\overline{t}_{\text{в}}}(k+1), \tag{9}$$

где выражение (6) – уравнение состояния показателя своевременности (оперативности) выявления отклонения в состоянии ИБ на $(k+1)$-м шаге функционирования SIEM-системы, в котором $\vec{t}_{\text{в}}(k+1)$ – вектор-столбец значений показателя своевременности (оперативности) выявления отклонения в состоянии ИБ на $(k+1)$-м шаге; $\mathrm{C}^{\text{т}}_{\overline{t}_{\text{в}}}(k+1)$ – транспонированная диагональная квадратная матрица (порядка m) возможных значений показателя своевременности (оперативности) выявления отклонения в состоянии ИБ на $(k+1)$-м шаге функционирования SIEM-системы, причем число m (строк и столбцов) зависит от выбранного числа состояний (глубины моделирования); $\vec{\Theta}_{\overline{t}_{\text{в}}}(k+1)$ – вспомогательный вектор-столбец индикаторов состояния показателя своевременности (оперативности), вводимый для удобства записи динамики перехода показателя своевременности (оперативности) из состояния в состояние. Выражения (7)–(9) имеют физический смысл, аналогичный выражениям (2), (3), и являются уравнением состояния вспомогательного вектора индикаторов, уравнением для определения приращений индикаторов состояния и уравнением наблюдения за процессом смены состояний среднего времени $\overline{t}_{\text{в}}(k)$ выявления отклонения в состоянии ИБ соответственно.

Методологическая часть

Вектор значений модифицированного возбуждающего шума $\vec{\vartheta}'(k+1)$, определяющий значения $\vec{\Theta}$ на $(k+1)$-м шаге (значения вспомогательных индикаторов процесса $x\,(k+1)$) формируются на основе сравнения с пороговыми значениями отклонений ПК процесса функционирования SIEM-системы выборочных значений БГШ $\vartheta^{\text{бгш}}_{m}(k)$, преобразованного в возбуждающий шум $\vartheta'_{m}(k+1)$ путем линейной процедуры

$$\vartheta'_m(k+1) = \left| \Gamma(k+1) \right| \vartheta^{\text{бгш}} + \Delta\varsigma_{\vartheta(k)} \begin{matrix} \text{"1"} \\ > \\ < \\ \text{"0"} \end{matrix} x_{\text{пор}\,m} \text{ при } \begin{cases} \mathrm{M}[\vartheta'(k+1)] = \Delta\varsigma_{\vartheta}(k), \\ \mathrm{D}[\vartheta'(k+1)] = \Gamma^2(k), \end{cases} \tag{10}$$

которая в матричной форме имеет вид

$$\begin{vmatrix} \vartheta'_1(k+1) \\ \vartheta'_2(k+1) \\ \vdots \\ \vartheta'_m(k+1) \end{vmatrix} = \begin{vmatrix} \Gamma_1(k) & 0 & \cdots & 0 \\ 0 & \Gamma_2(k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Gamma_m(k) \end{vmatrix} \begin{vmatrix} \vartheta_1^{\text{бгш}}(k) \\ \vartheta_2^{\text{бгш}}(k) \\ \vdots \\ \vartheta_m^{\text{бгш}}(k) \end{vmatrix} + \begin{vmatrix} \Delta\varsigma_{\vartheta_1}(k) \\ \Delta\varsigma_{\vartheta_2}(k) \\ \vdots \\ \Delta\varsigma_{\vartheta_m}(k) \end{vmatrix}, \tag{11}$$

где $\Delta\varsigma_{\vartheta_m}(k)$ – приращения математического ожидания формируемого процесса, полученные на основе априорных данных о цепи Маркова, по отношению к матожиданию БГШ, возбуждающего этот процесс; $\Gamma_m(k) = T\sqrt{2\sigma_\Theta^2 q_{mm}/N_{\vartheta_m}}$ – коэффициент, предназначенный для коррекции дисперсии гауссовского шума на основе априорных данных о цепи Маркова для данного шага; $\left|\Gamma(k)\right| = G(t)T = diag\,\{T\sqrt{2\sigma_\Theta^2 q_{mm}/N_{\vartheta_m}}\}$ – матрица диффузии (возбуждения) процесса $\vec{\Theta}(k)$; σ_Θ^2 – дисперсия процесса $\vec{\Theta}(k)$; q_{mm} – элементы матрицы интенсивностей перехода вспомогательных индикаторов состояния $\vec{\Theta}(k)$ процесса функционирования SIEM-системы; M – символ математического ожидания формируемого процесса на (k + 1)-м шаге; D – символ дисперсии формируемого процесса на (k + 1)-м шаге; Γ (k + 1) – коэффициент, предназначенный для коррекции дисперсии на (k + 1)-м шаге; $x_{\text{пор}\,m}$ – граничное, «пороговое» значение конкретного m-го состояния ПК; $\Gamma^2(k)$ – символ взятия в квадрат коэффициента, предназначенный для коррекции дисперсии гауссовского шума.

Рассмотрим детально шаги (этапы) методологии определения элементов вектора компенсационных добавок в уравнении состояния данной модифицированной модели системы управления информацией и событиями безопасности с учетом преобразования шума возбуждения.

Результаты анализа (на основе априорных данных о цепи Маркова), к какому состоянию «стремится» процесс на следующем шаге, дают нам решающее правило для выбора вектора компенсационных добавок и, в конечном итоге, для определения значений элементов вектора вспомогательных индикаторов состояния $\vec{\Theta}_m(k+1)$ процесса функционирования SIEM-системы.

Вычисление значений $\Delta\varsigma_{\vartheta_m}(k)$, корректирующих вероятности состояния исходного шума возбуждения $\vartheta^{\text{бгш}}(k)$, может быть осуществлено для случая однородной цепи априорно, на основе выражения

$$\Delta\varsigma_{\vartheta_m}(k) = (1 - p_m(\varsigma_{\vartheta_m}(k)))^{-1} = \Phi^{-1}(-\varsigma_{\vartheta_m}(k)), \tag{12}$$

где (–1) – символ взятия обратной функции; $\Phi(\varsigma_{\vartheta_m}(k)) = 1 - \Phi(-\varsigma_{\vartheta_m}(k))$ – интеграл вероятности; $p_m(\varsigma_{\vartheta_m}(k))$ – вероятность принятия процессом значения $\vartheta'_m > 0$, численно равная вероятности принятия процессом Θ_m значения $\Theta_m(k+1) = 1$:

$$p_m(\varsigma_{\vartheta_m}(k)) = p_m(k) = \sum_{i=1}^{M} p_i(k-1)\, p_{im}(k-1 \,|\, k), \quad m = \overline{1, M}, \tag{13}$$

где M – количество состояний процесса; i – текущее i-е состояние процесса, где $i = 1, \ldots, m, \ldots, M$; $p_i(k-1)$ – вероятность того, что на предыдущем (k – 1)-м шаге процесс находился в i-ом состоянии; $p_{im}(k - 1/k)$ – вероятность перехода процесса из i-го состояния на предыдущем (k – 1)-м шаге в m-ое состояние на нынешнем k-ом шаге.

Вычисление значений коэффициента $\Gamma_m(k)$, предназначенного для коррекции дисперсии случайных дискретных реализаций исходного БГШ $\vartheta^{\text{бгш}}(k)$, происходит следующим образом. Учитывая, что спектральная плотность мощности шума возбуждения $\vartheta'(k)$ связана с его дисперсией выражением $N_\vartheta = \sigma_\vartheta^2 T$, где N_ϑ – коэффициент спектральной плотности мощности шума возбуждения; T – обозначение такта, отрезка времени, временного эквивалента одного шага k процесса, за которое процесс может изменить свое состояние; а интенсивность перехода процесса $\Theta(k)$ из состояния в состояние – с соответствующими вероятностями – выражением $q_{mm} = p_{mm} / T$, где p_{mm} – элементы матрицы вероятностей перехода процесса $\Theta(k)$ из состояния в состояние, уравнение для коэффициента $\Gamma_m(k)$ может быть записано в виде

$$\Gamma_m(k) = 2\ p_{mm}(k). \tag{14}$$

Если выбранное с учетом введенных коэффициентов значение модифицированного шума возбуждения $\vartheta'_m(k+1)$ попадает в границы допусков $-\Delta\varsigma_\vartheta \le \vartheta'_m(k+1) \le +\Delta\varsigma_\vartheta$ (что показывает «стремление» Θ_m на $(k+1)$-м шаге к 1), в уравнении (3) принимается решение о том, что элемент вектора компенсационных добавок $\vartheta'_m(k)$ – положительный, а остальные элементы этого вектора – отрицательны, что при решении уравнения (2) дает нам $\Theta_m(k+1) = 1$. Формирование текущих значений матрицы компенсационных добавок $\vartheta(k)$ происходит в соответствии с правилом: если процесс описывается двумя состояниями Θ_0 и Θ_1 (т. е. $m = \overline{1, 2}$), то вектор последовательностей возбуждения для определения значения вспомогательного индикатора состояния Θ_1 процесса функционирования SIEM-системы находится из матрицы

$$\vartheta_1(k) = \begin{vmatrix} \vartheta_1^{11}(k) & \vartheta_1^{12}(k) \\ \vartheta_1^{21}(k) & \vartheta_1^{22}(k) \end{vmatrix} = \begin{vmatrix} -p_{12}(k) & (1-p_{12}(k)) \\ -p_{21}(k) & (1-p_{21}(k)) \end{vmatrix}; \tag{15}$$

если для описания процесса смены состояний ПК функционирования SIEM-системы используем три и более состояния Θ_m (т. е. $m = 1, 2, \ldots, M$), то выбор матрицы компенсационных добавок для m-го состояния $\vartheta_m(k)$ (на первом этапе решения уравнения (3)) и вектора компенсационных добавок из этой матрицы $\vec{\vartheta}_m$ (на втором этапе решения уравнения (3)) происходит из блочной диагональной матрицы вида

$$\left\|\vartheta(k)\right\| = \begin{vmatrix} \left|\vartheta_1(k)\right| & 0 & \cdots & 0 \\ 0 & \left|\vartheta_2(k)\right| & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \left|\vartheta_m(k)\right| \end{vmatrix}. \tag{16}$$

Элементы матриц текущих компенсационных добавок $\vartheta_m(k)$ для различных состояний ПК процесса функционирования SIEM-системы находятся в соответствии с правилом

$$\begin{aligned} \left|\vartheta_m(k)\right| &= \begin{vmatrix} \vartheta_{11}(k) & \vartheta_{21}(k) & \vartheta_{31}(k) & \cdots & \vartheta_{m1}(k) \\ \vartheta_{12}(k) & \vartheta_{22}(k) & \vartheta_{32}(k) & \cdots & \vartheta_{m2}(k) \\ \vartheta_{13}(k) & \vartheta_{23}(k) & \vartheta_{33}(k) & \cdots & \vartheta_{m3}(k) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vartheta_{1m}(k) & \vartheta_{2m}(k) & \vartheta_{3m}(k) & \cdots & \vartheta_{m}(k) \end{vmatrix} = \\ &= \begin{vmatrix} (1-p_{m1}(k)) & -p_{m1}(k) & -p_{m1}(k) & \cdots & -p_{m1}(k) \\ -p_{m2}(k) & (1-p_{m2}(k)) & -p_{m2}(k) & \cdots & -p_{m2}(k) \\ -p_{m3}(k) & -p_{m3}(k) & (1-p_{m3}(k)) & \cdots & -p_{m3}(k) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -p_{mm}(k) & -p_{mm}(k) & -p_{mm}(k) & \cdots & (1-p_{mm}(k)) \end{vmatrix}. \end{aligned} \tag{17}$$

Количество состояний m определяется исходя из требуемой точности оценивания ПК процесса функционирования SIEM-системы. Оптимизация размерности пространств состояния и наблюдения процесса функционирования SIEM-системы с учетом требований к допустимой погрешности оценивания представляет собой отдельную теоретическую и практическую задачу. Окончательным результатом решения уравнения (3) является вектор $\vec{\vartheta}_m(k)$, содержащий компенсирующие добавки для каждого рассматриваемого m-го состояния ПК SIEM-системы:

$$\vec{\vartheta}_m(k) = \begin{vmatrix} \vartheta_{m1}(k) \\ \vartheta_{m2}(k) \\ \vartheta_{m3}(k) \\ \vdots \\ \vartheta_{mm}(k) \end{vmatrix}. \qquad (18)$$

Таким образом, показано, что предложенный методологический подход позволяет определять значения приращения математического ожидания моделируемого процесса, полученные на основе априорных данных о цепи Маркова, по отношению к математическому ожиданию БГШ, возбуждающего этот процесс. Этот подход сочетает вычисление значений приращения математического ожидания формируемого процесса и значений коэффициента, предназначенного для коррекции дисперсии случайных дискретных реализаций исходного БГШ, и позволяет принимать решение о том, какие значения будут принимать элементы вектора (18) в уравнении состояния данной модифицированной модели SIEM-системы с учетом преобразования шума возбуждения.

Заключение

Таким образом, выражениями (1)–(5) и (10)–(18) описан вариант модели процесса функционирования SIEM-системы. Эта модель представляет собой формализованное аналитическое описание, в терминах марковской цепи в форме разностных стохастических уравнений (1)–(4), динамики смены состояний показателей качества, характеризующих существенные свойства процесса функционирования SIEM-системы, в пространстве состояний.

В статье решена научная задача, заключавшаяся в усовершенствовании (модификации) алгоритмов преобразования шума возбуждения, используемого в модели. Описан новый механизм определения значений приращения математического ожидания моделируемого процесса, полученных на основе априорных данных о цепи Маркова, по отношению к математическому ожиданию белого гауссовского шума, возбуждающего этот процесс. Преобразование шума возбуждения служит для получения приращений математического ожидания моделируемого процесса, помогает определить эти приращения нецелочисленных значений индикаторов состояния. Полученные математические ожидания определяют «тренд», направление (ближе к 0 или 1) движения индикатора состояния ПК в пространстве состояний. В сущности, этот механизм позволяет, опираясь на несложные вычисления, принимать решение о том, какие значения будут принимать элементы вектора компенсационных добавок в уравнении состояния вспомогательного вектора индикаторов данной модифицированной модели с учетом преобразования шума возбуждения. Это позволяет упростить модель, снизить ее вычислительную сложность без существенных потерь в точности (адекватности).

Практическое применение усовершенствованной модели возможно как в рамках исследовательских работ, так и в системах автоматизированного контроля информационной безопасности. Направлением дальнейших исследований может быть разработка модели, учитывающей как количественный, так и качественный (например, описываемый с помощью лингвистических переменных, типичных для нечетких множеств) характер показателей качества.

СПИСОК ЛИТЕРАТУРЫ

1. *Kizza J. M.* Guide to Computer Network Security. New York: Springer, 2015. 545 p.

2. *Sun Y.* Research on Security Issues and Protection Strategy of Computer Network // The Open Automation and Control Systems Journal. 2015. N. 7. P. 2097–2101.

3. *Dordal P. L.* An Introduction to Computer Networks. Release 1.9.0. January 27, 2017, 745 p. URL: https://archive.org/details/academictorrents_958e2487d2db5f41f9c056bb35cf547edf38528f/mode/2up (дата обращения: 22.12.2019).

4. *Pfleeger C. P., Pfleeger S. L.* Security in Computing. New Jersey: Prentice Hall, 2015. 944 p.

5. *Miller D. R., Harris S., Vandyke S.* Security Information and Event Management (SIEM) Implementation. New York: McGrawHill, 2011. 430 p.

6. *Kotenko I. V., Parashchuk I. B.* Synthesis of controlled parameters of cyber-physical-social systems for monitoring of security incidents in conditions of uncertainty // Journal of Physics: Conference Series, IOP Publishing. 2018. N. 1069 (1): 012153. P. 1–6.

7. *Kotenko I. V., Doynikova E. V.* Countermeasure selection in SIEM systems based on the integrated complex of security metrics // Proceedings of the 23th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP 2015). IEEE Computer Society, 2015. P. 567–574.

8. *La Padula L. J.* Secure Computer Systems: A Mathematical Model // MTR-2547. Massachusetts: The MITRE Corporation, Bedford, 1993. V. I. 33 p.

9. *Higham D. J.* An Algorithmic Introduction to Numerical Simulation of Stochastic Differential Equations // SIAM REVIEW. 2001. N. 43 (3). P. 525–546.

10. *Iacus S. M.* Simulation and Inference for Stochastic Differential Equations: With R Examples. New York: Springer Verlag, 2008. 214 p.

11. *Yuksel S.* Control of Stochastic Systems // Queen's University Mathematics and Engineering and Mathematics and Statistics. 2017. 167 p.

12. *Van Handel R.* Stochastic Calculus, Filtering and Stochastic Control. New York, Springer, 2007. 261 p.

13. *Oksendal B.* Stochastic Differential Equations. An introduction with applications. Berlin Heidelberg, Springer Verlag, 2007. 311 p.

14. *Stewart N. E., Thomas G. K.* Markov processes: Characterization and Convergence. Wiley Series in Probability and Statistics. New York, John Wiley & Sons Inc., 1986. P. 214–234.

15. *Bini D., Latouche G., Meini B.* Numerical Methods for Structured Markov Chains. New York: Oxford University Press, 2005. 215 p.

16. *Dobre T. Gh., Marcano J. G. S.* Chemical Engineering: Modelling, Simulation and Similitude. Weinheim: Wiley-VCH, 2007. 568 p.

17. *Oliver D., Kelliher T., Keegan J.* Engineering Complex Systems With Models and Objects. New York: McGraw-Hill, 2007. 340 p.

18. *Quarteroni A.* Mathematical Models in Science and Engineering // Proc. of Notices of the AMS. 2009. V. 56. N. 1. P. 9–19.

19. *Tweedie R. L.* Drift conditions and invariant measures for Markov chains // Stochastic Processes and Their Applications. 2001. V. 1. P. 345–354.

20. *Kotenko I. V.*, *Parashchuk I. B.* Determining the Parameters of the Mathematical Model of the Process of Searching for Harmful Information // Cyber-Physical Systems: Industry 4.0 Challenges. Studies in Systems, Decision and Control 260. A. G. Kravets et al. (eds.). Springer Nature Switzerland AG 2020, 2019. P. 225–236.

21. *Kotenko I. V.*, *Parashchuk I. B.* An approach to modeling the decision support process of the security event and incident management based on Markov chains // 9th IFAC Conference on Manufacturing Modelling, Management and Control (MIM-2019) (Berlin, Germany, 28–30 August 2019). IFAC-PapersOnLine, 2019. V. 52. Iss. 13. P. 934–939.

Статья поступила в редакцию 17.01.2020

ИНФОРМАЦИЯ ОБ АВТОРАХ

Котенко Игорь Витальевич – Россия, 199178, Санкт-Петербург; Санкт-Петербургский институт информатики и автоматизации Российской академии наук; д-р техн. наук, профессор, зав. лабораторией проблем компьютерной безопасности; ivkote@comsec.spb.ru.

Паращук Игорь Борисович – Россия, 199178, Санкт-Петербург; Санкт-Петербургский институт информатики и автоматизации Российской академии наук; д-р техн. наук, профессор; ведущий научный сотрудник лаборатории проблем компьютерной безопасности; shchuk@rambler.ru.

MODEL OF SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM

I. V. Kotenko, I. B. Parashchuk

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Saint-Petersburg, Russian Federation

Abstract. The article is focused on the development of a mathematical model of functioning the security information and event management system known as the SIEM system. This model is a formalized analytical description (in terms of a Markov chain in the form of stochastic differential equations) of the dynamics of the changing states of quality indicators characterizing the essential properties of functioning the security information and events management system in the state space. The model is a system of equations of state and observation, traditional for the Markov chain in the form of finite differences. The scientific task is to improve (modify) the algorithms for converting excitation noise used in the model. A mechanism is proposed for determining the values of the mathematical expectation increment of the simulated process, obtained on the basis of a priori data on the Markov chain, in relation to the mathematical expectation of white Gaussian noise exciting this process. Based on simple calculations the mechanism helps to decide what values can be taken by the elements of the vector of compensation additives in the equation of state of the auxiliary indicator vector of this modified model, taking into account the conversion of the excitation noise. This allows simplifying the model and reducing its computational complexity without significant losses in accuracy (adequacy). The practical application of an improved model is possible both in the framework of the research and in the systems of automated control of information security.

Key words: mathematical expectation, system of security information and event management, quality indicator, functioning process, matrix, state.

For citation: Kotenko I. V., Parashchuk I. B. Model of security information and event management system. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2020;2:84-94. (In Russ.) DOI: 10.24143/2072-9502-2020-2-84-94.

REFERENCES

1. Kizza J. M. *Guide to Computer Network Security*. New York, Springer, 2015. 545 p.
2. Sun Y. Research on Security Issues and Protection Strategy of Computer Network. *The Open Automation and Control Systems Journal*, 2015, no. 7, pp. 2097-2101.
3. Dordal P. L. *An Introduction to Computer Networks. Release 1.9.0*. January 27, 2017, 745 p. Available at: https://archive.org/details/academictorrents_958e2487d2db5f41f9c056bb35cf547edf38528f/mode/2up (accessed: 22.12.2019).
4. Pfleeger C. P., Pfleeger S. L. *Security in Computing*. New Jersey, Prentice Hall, 2015. 944 p.
5. Miller D. R., Harris S., Vandyke S. *Security Information and Event Management (SIEM) Implementation*. New York, McGrawHill, 2011. 430 p.
6. Kotenko I. V., Parashchuk I. B. Synthesis of controlled parameters of cyber-physical-social systems for monitoring of security incidents in conditions of uncertainty. *Journal of Physics: Conference Series, IOP Publishing*, 2018, no. 1069 (1): 012153, pp. 1-6.
7. Kotenko I. V., Doynikova E. V. Countermeasure selection in SIEM systems based on the integrated complex of security metrics. *Proceedings of the 23th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2015). IEEE Computer Society*, 2015, pp. 567-574.
8. La Padula L. J. *Secure Computer Systems: A Mathematical Model. MTR-2547*. Massachusetts: The MITRE Corporation, Bedford, 1993. Vol. I. 33 p.
9. Higham D. J. An Algorithmic Introduction to Numerical Simulation of Stochastic Differential Equations. *SIAM REVIEW*, 2001, no. 43 (3), pp. 525-546.
10. Iacus S. M. *Simulation and Inference for Stochastic Differential Equations. With R Examples*. New York, Springer Verlag, 2008. 214 p.
11. Yuksel S. *Control of Stochastic Systems*. Queen's University Mathematics and Engineering and Mathematics and Statistics, 2017. 167 p.
12. Van Handel R. *Stochastic Calculus, Filtering and Stochastic Control*. New York, Springer, 2007. 261 p.
13. Oksendal B. *Stochastic Differential Equations. An introduction with applications*. Berlin Heidelberg, Springer Verlag, 2007. 311 p.

14. Stewart N. E., Thomas G. K. *Markov processes: Characterization and Convergence. Wiley Series in Probability and Statistics.* New York: John Wiley & Sons Inc., 1986. Pp. 214-234.

15. Bini D., Latouche G., Meini B. *Numerical Methods for Structured Markov Chains*. New York, Oxford University Press, 2005. 215 p.

16. Dobre T. Gh., Marcano J. G. S. *Chemical Engineering: Modelling, Simulation and Similitude*. Weinheim, Wiley-VCH, 2007. 568 p.

17. Oliver D., Kelliher T., Keegan J. *Engineering Complex Systems With Models and Objects*. New York, McGraw-Hill, 2007. 340 p.

18. Quarteroni A. Mathematical Models in Science and Engineering. *Proceedings of Notices of the AMS*, 2009, vol. 56, no. 1, pp. 9-19.

19. Tweedie R. L. Drift conditions and invariant measures for Markov chains. *Stochastic Processes and Their Applications*, 2001, vol. 1, pp. 345-354.

20. Kotenko I. V., Parashchuk I. B. *Determining the Parameters of the Mathematical Model of the Process of Searching for Harmful Information. Cyber-Physical Systems: Industry 4.0 Challenges. Studies in Systems, Decision and Control 260.* A. G. Kravets et al. (eds.). Springer Nature Switzerland AG 2020, 2019. Pp. 225-236.

21. Kotenko I. V., Parashchuk I. B. An approach to modeling the decision support process of the security event and incident management based on Markov chains. *9th IFAC Conference on Manufacturing Modelling, Management and Control (MIM-2019) (Berlin, Germany, 28–30 August 2019). IFAC-PapersOnLine*, 2019, vol. 52, iss. 13, pp. 934939.

The article submitted to the editors 17.01.2020

INFORMATION ABOUT THE AUTHORS

Kotenko Igor Vitalievich – Russia, 199178, Saint-Petersburg; St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences; Doctor of Technical Sciences, Professor; Head of the Laboratory of Computer Security Problems; ivkote@comsec.spb.ru.

Parashchuk Igor Borisovich − Russia, 199178, Saint-Petersburg; St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences; Doctor of Technical Sciences, Professor; Leading Researcher of the Laboratory of Computer Security Problems; shchuk@rambler.ru.