Методика оценки эффективности систем обработки сетевого контента для обнаружения вредоносной информации с учетом устранения неопределенности смыслового наполнения информационных объектов

В. А. Десницкий
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН);
desnitsky@comsec.spb.ru

И. В. Котенко[1], И. Б. Паращук[2]
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН);
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
[1]ivkote@comsec.spb.ru, [2]parashchuk@comsec.spb.ru

***Аннотация*. Предложена модель, построенная на основе марковских цепей и учитывающая вероятностно-временной механизм изменения состояния процесса функционирования систем обработки сетевого контента в динамике. Эта модель призвана математически описывать процесс смены состояний показателей (признаков) вредоносной информации, которая должна быть обнаружена в рамках функционирования систем такого класса. Разработана методика многокритериальной динамической оценки эффективности систем обработки сетевого контента. Методика основана на анализе текущих отклонений значений показателей вредоносной информации от требований к ним, учитывает и устраняет неопределенность смыслового наполнения информационных объектов. Методика позволяет также учитывать переходные процессы при введении управлений структурой, параметрами и режимами работы таких систем в различных условиях.**

Ключевые слова: система обработки; сетевой контент; эффективность; показатель; вредоносная информация; вероятность; неопределенность

I. Введение

Одной из основных проблем построения интеллектуальных систем обработки сетевого контента (СОСК) является анализ эффективности их функционирования. Результаты такого анализа позволяют оперативно вводить адекватные управляющие воздействия, направленные на поиск, обнаружение и противодействие вредоносной информации (ВИ). За эти функции в СОСК отвечают механизмы интеллектуального анализа смыслового наполнения информационных объектов. Оценивание эффективности функционирования сложных систем, в том числе и систем обработки сетевого контента (СОСК), требует большого числа знаний об этих системах и процессах, реализуемых ими. Эти знания могут быть выражены количественно, но могут быть экспериментальными и экспертными.

При этом существует объективная неопределенность, связанная с исходными данными, необходимыми как для интеллектуального анализа смыслового наполнения информационных объектов, так и для анализа эффективности СОСК в целом. Особенно это актуально при современных угрозах безопасности и алгоритмах агрессивного внедрения ВИ, когда возможны сложные многошаговые атаки и «внедрения» ВИ со стороны различных категорий нарушителей [1, 2]. Для моделирования сложных систем, таких как СОСК, и обработки неопределенных знаний в последнее время широко используются вероятностно-временные модели смены состояний показателей ВИ совместно с алгоритмами устранения неопределенности знаний (данных) об этих состояниях. Решение подобных задач в комплексе целесообразно и актуально. Это позволяет: использовать данные методы в комплексе для описания элементов задач моделирования СОСК (в интересах оценки ее эффективности) и оценивания показателей ВИ; формализовать и устранить неопределенность смыслового наполнения информационных объектов с помощью алгоритмов дополнительной идентификации показателей ВИ; автоматически накапливать знания о свойствах СОСК и принимать оптимальные решения по обнаружению ВИ, опираясь на накопленные знания и полученные результаты анализа эффективности систем такого класса.

II. Релевантные работы

Разработке математических моделей и методик оценки эффективности сложных управляемых технических систем посвящено много работ. Существует ряд частных методик

Это исследование было поддержано грантом РНФ (проект № 18-11-00302) в СПИИРАН.

оценки эффективности функционирования информационных систем, систем защиты, хранения и аналитической обработки информации [3–14]. Вместе с тем, дальнейшее использование частных методик оценки эффективности для сравнительного анализа существующих СОСК и выработки перспективных направлений их развития становится затруднительным в силу ряда причин. Во-первых, существующие частные модели и методики не учитывают специфические свойства и современные технологии работы интеллектуальных СОСК, не учитывают особенности показателей ВИ, которые необходимо анализировать [3–5]. Во-вторых, учет переходных процессов, присущих различным состояниям параметров ВИ и многокритериальный характер требований, предъявляемых к анализу смыслового наполнения информационных объектов, приводят к постановке не только векторной, но и многокритериальной задачи анализа эффективности функционирования интеллектуальных СОСК [6–8]. В-третьих, существующие методики оценки эффективности информационных систем, систем защиты, хранения и аналитической обработки информации, рассчитаны на анализ в условиях локальной стационарности, в статике [9–11]. Помимо этого, решение проблемы анализа эффективности систем аналитической обработки информации для обнаружения ВИ до недавнего времени базировалось на многомерной совместной плотности распределения вероятностей (ПРВ) значений показателей ВИ, определяемой на основе сбора и обработки большого объема статистических данных [12–14]. Все это делает актуальной задачу развития существующих методик и поиск новых математических методов анализа эффективности СОСК в рамках вероятностного подхода. Необходима методика, позволяющая сократить размерность задачи многокритериального динамического анализа эффективности функционирования СОСК.

III. Теоретическая часть

С целью развития существующих методик на случай динамического анализа эффективности функционирования современных СОСК, предложен переход от стационарных вероятностных моделей показателей ВИ, подлежащих контролю в рамках таких систем, к вероятностно-временным моделям показателей ВИ (ПВИ) на основе математического аппарата управляемых цепей Маркова, представляемых в форме разностных стохастических уравнений. Вероятностно-временные модели ПВИ, обнаруживаемых СОСК, аналитические модели процесса функционирования СОСК и ее элементов (например, подсистем анализа смыслового наполнения информационных объектов) на основе математического аппарата управляемых цепей Маркова в форме разностных стохастических уравнений, позволяют, в отличие от существующих, учесть динамику вероятностно-временного механизма изменения состояния СОСК и коррелированность оценок на соседних τ – тактах (шагах) функционирования данной системы в условиях различного вида воздействий. При этом вероятностно-временная модель отдельно взятого ПВИ, обнаруживаемого СОСК (имеющего смысл отклонения $\Delta\vec{v}$ какого-либо ПВИ от требуемых значений в процессе функционирования системы) на основе математического аппарата управляемых цепей Маркова, представляемых в форме разностных стохастических уравнений, имеет вид:

$$\Delta\vec{v}(\tau+1) = \mathrm{C}^{\mathrm{T}}(\tau+1)\,\vec{\Phi}(\tau+1); \quad (1)$$

$$\vec{\Phi}(\tau+1) = \xi^{\mathrm{T}}(\tau+1,\tau,u)\,\vec{\Phi}(\tau) + \vec{\eta}(\tau); \quad (2)$$

$$\vec{\eta}(\tau) = [\eta^{\mathrm{T}}(\tau)\vec{\Phi}(\tau)]\vec{\eta}'(\tau+1); \quad (3)$$

$$\vec{Y}(\tau+1) = \mathrm{H}(\tau, v(\tau))\,\vec{\Phi}(\tau+1) + \vec{\omega}(\tau+1), \quad (4)$$

где выражение (1) – уравнение состояния процесса $\Delta\vec{v}$ на (τ+1)-ом такте (в нашем случае это состояние отклонения некоторого параметра ВИ), в котором: $\mathrm{C}^{\mathrm{T}}(\tau+1)$ – транспонированная матрица-строка возможных значений отклонений параметра ВИ; $\vec{\Phi}(\tau+1)$ – вспомогательный вектор индикаторов состояния параметра ВИ в виде отклонений. Выражение (2) – уравнение состояния вспомогательного вектора индикаторов, в котором: $\xi^{\mathrm{T}}(\tau+1,\tau,u)$ – транспонированная матрица вероятностей перехода процесса, обуславливающего смену состояний ПВИ, контролируемых (обнаруживаемых) СОСК; $\vec{\Phi}(\tau)$ – вектор значений индикаторов состояния на предыдущем такте (шаге); $\vec{\eta}(\tau)$ – вектор компенсационных добавок, элементы которого предназначены для компенсации нецелочисленной части уравнения (2) и получены в результате коррекции исходного шума возбуждения – белого гауссовского шума (БГШ). В выражении (3), описывающем вектор компенсационных добавок, $\eta^{\mathrm{T}}(\tau)$ – транспонированная диагональная блочная матрица компенсационных добавок, являющаяся ступенчатым мартингалом, элементы которого предназначены для компенсации нецелочисленной части в уравнении (2); $\vec{\eta}'(\tau+1)$ – вектор значений модифицированного возбуждающего шума, определяющий значения $\vec{\Phi}$ на (τ+1)-ом такте. Использование аппарата управляемых цепей Маркова в форме разностных стохастических уравнений позволяет построить аналитические модели процессов функционирования сложной информационной системы (в нашем случае СОСК). Эти модели учитывают динамический и вероятностный характер, нестационарность как самих процессов функционирования систем такого класса [15, 16], так и процессов управления ими, процессов обнаружения ВИ путем интеллектуального анализа смыслового наполнения информационных объектов. Кроме того, применение положений теории переменных состояния позволяет выразить в форме разностных стохастических уравнений на основе динамических моделей ПВИ как частные процессы, так и подсистемы, их реализующие. Именно поэтому обобщенный показатель эффективности может включать эффективность процессов обнаружения ВИ и управления, а также эффективность процессов функционирования отдельных элементов СОСК – подсистемы анализа смыслового наполнения информационных объектов (ПАСН) и подсистемы управления (ПСУ) СОСК. Это, в конечном итоге, позволяет получать значения текущих частных показателей эффективности функционирования (ЧПЭФ) и текущего обобщенного показателя

эффективности функционирования (ОПЭФ) СОСК в виде совместной вероятности выполнения требований, предъявляемых пользователем к качеству функционирования систем такого класса на (τ+1)-ом такте:

$$\begin{aligned} P_{\text{вып тр}}(\tau+1) &= P(\tau+1)[(\vec{S}_{\text{ф}}(\tau) \le \vec{S}_{\text{ф}}^{\text{тр}})/(\vec{S}_{\text{СОСК}}^{\text{тр}})] = \\ &= P_{\text{вып оВИ}}(\tau+1)[(\vec{S}_{\text{оВИ}}(\tau+1) \le \vec{S}_{\text{оВИ}}^{\text{тр}})/(\vec{S}_{\text{у}}(\tau+1) \le \vec{S}_{\text{у}}^{\text{тр}}) \bigcap \\ &\bigcap (\vec{S}_{\text{ПАСН}}(\tau+1) \le \vec{S}_{\text{ПАСН}}^{\text{тр}}) \bigcap (\vec{S}_{\text{ПСУ}}(\tau+1) \le \vec{S}_{\text{ПСУ}}^{\text{тр}})] \times \\ &\times P_{\text{вып у}}(\tau+1)[(\vec{S}_{\text{у}}(\tau+1) \le \vec{S}_{\text{у}}^{\text{тр}})/ \\ &/(\vec{S}_{\text{ПАСН}}(\tau+1) \le \vec{S}_{\text{ПАСН}}^{\text{тр}}) \bigcap (\vec{S}_{\text{ПСУ}}(\tau+1) \le \vec{S}_{\text{ПСУ}}^{\text{тр}})] \times \\ &\times P_{\text{вып ПАСН}}(\tau+1)[(\vec{S}_{\text{ПАСН}}(\tau+1) \le \vec{S}_{\text{ПАСН}}^{\text{тр}})/ \\ &/(\vec{S}_{\text{ПСУ}}(\tau+1) \le \vec{S}_{\text{ПСУ}}^{\text{тр}})] \times \\ &\times P_{\text{вып ПСУ}}(\tau+1)[(\vec{S}_{\text{ПСУ}}(\tau+1) \le \vec{S}_{\text{ПСУ}}^{\text{тр}})]; \end{aligned} \quad (5)$$

где $P_{\text{вып оВИ}}(\tau+1)$, $P_{\text{вып ПАСН}}(\tau+1)$, $P_{\text{вып у}}(\tau+1)$ – условные вероятности выполнения требований к качеству процесса обнаружения ВИ (ПВИ), ПАСН и процесса управления на (τ+1)-ом такте (шаге) функционирования СОСК, определяемые при условии выполнения требований к текущим показателям качества ПСУ СОСК; $P_{\text{вып ПСУ}}(\tau+1)$ – безусловная вероятность выполнения требований к качеству ПСУ СОСК на (τ+1)-ом такте (шаге) функционирования СОСК. Условные и безусловная вероятности выполнения требований в выражении (5) содержат соотношения истинных $\vec{S}$ и требуемых $\vec{S}^{\text{тр}}$ значений элементов вектора ПВИ (процесса обнаружения ВИ) $\vec{S}_{\text{оВИ}}(\tau+1)$, вектора показателей качества процесса управления $\vec{S}_{\text{у}}(\tau+1)$, ПАСН $\vec{S}_{\text{ПАСН}}(\tau+1)$ и ПСУ $\vec{S}_{\text{ПСУ}}(\tau+1)$ соответственно. При этом частные показатели эффективности имеют тот же смысл, что и в работах [15, 17, 18], но развиты на случай динамического анализа эффективности функционирования СОСК с точки зрения обнаружения вредоносной информации.

IV. Методологическая часть (методика)

Сформулируем и рассмотрим сущность этапов методики оценки эффективности систем обработки сетевого контента для обнаружения вредоносной информации с учетом устранения неопределенности смыслового наполнения информационных объектов. Отличительной особенностью предложенной методики, помимо сокращения размерности задачи анализа, является получение вероятностных ЧПЭФ. Это реализуется путем интегрирования текущих одномерных плотностей распределения вероятностей (ПРВ), формируемых на основе оценочных значений числовых характеристик показателей качества обнаружения ВИ (ПВИ), управления и показателей качества подсистем СОСК. Текущее оценивание конкретного частного показателя качества СОСК предполагается осуществлять с использованием алгоритмов оптимальной нелинейной фильтрации наблюдаемых компонент этого показателя качества. Затем, оценочные значения конкретного частного показателя качества используются для формирования текущей ПРВ значений этого показателя с последующим интегрированием полученной ПРВ по его пороговым значениям. Далее происходит свертка полученных ЧПЭФ в пошаговые значения ОПЭФ в соответствии с выражением (5). Таким образом, методика оценки эффективности систем обработки сетевого контента для обнаружения вредоносной информации с учетом устранения неопределенности смыслового наполнения информационных объектов включает несколько этапов:

1. Сбор (моделирование) статистических данных о системе показателей ВИ и показателях качества СОСК в целом за период наблюдения (такт функционирования)

$$\begin{aligned} \vec{S}_j(\tau+1) &= f(\Delta s_1(\tau+1), \ldots, \Delta s_i(\tau+1), \ldots, \Delta s_N(\tau+1)); \\ \vec{Y}_{\vec{S}_j}(\tau+1) &= \{y_{\Delta s_1}(\tau+1), \ldots, y_{\Delta s_N}(\tau+1)\}^{\text{т}} = \\ &\left\|\text{H}(\tau+1)\right\| \vec{\Phi}(\tau+1) + \vec{\omega}(\tau+1), \end{aligned} \quad (6)$$

где $\vec{S}_j(\tau+1)$ – вектор показателей качества j-го процесса СОСК (или подсистемы его обеспечивающей, например ПАСН или ПСУ) на (τ+1)-ом такте (шаге) функционирования; $\Delta s_i(\tau+1)$ – отклонения i-го компонента вектора показателей ВИ или иных показателей качества СОСК от требуемых значений на этом же такте; $\vec{Y}_{\vec{S}_j}(\tau+1)$ – вектор наблюдений за $\vec{S}_j(\tau+1)$, содержащий наблюдения за отклонениями отдельных i-ых показателей ВИ и иных показателей качества СОСК; $\left\|\text{H}(\tau+1)\right\|$ – матрица наблюдений за состоянием $\vec{S}_j(\tau+1)$; $\vec{\omega}(\tau+1)$ – вектор шумов наблюдения за процессом смены состояний $\vec{S}_j(\tau+1)$.

2. Оптимальная (по минимуму среднего квадратичного отклонения) фильтрация значений показателей наблюдаемого процесса смены состояний показателей ВИ и других показателей $\vec{S}_j(\tau+1)$:

$$\begin{aligned} &\{\Delta\hat{s}_1(\tau+1), \ldots, \Delta\hat{s}_i(\tau+1), \ldots, \Delta\hat{s}_N(\tau+1)\}^{\text{т}}; \\ &\Delta\hat{s}_1(\tau+1) = \text{M}\{\Delta\hat{s}_i(\tau+1)/y_{\Delta\hat{s}_i}(\tau+1)\}; \left\|\text{D}\right\|, i = \overline{1, N}, \end{aligned} \quad (7)$$

где $\Delta\hat{s}_1(\tau+1)$ – оценочное значение отклонения i-го показателя ВИ или иного показателя качества СОСК на (τ+1)-ом такте (шаге) ее функционирования. Это значение определяется как условное по наблюдениям оценочное значение моментов – математического ожидания (M) и дисперсии (D) процесса смены состояния i-го показателя ВИ на данном такте.

3. Формирование оценочного значения j-го текущего частного показателя качества СОСК $\hat{\vec{S}}_j(\tau+1)$ на основе оценочных значений его компонент:

$$\hat{\vec{S}}_j(\tau+1) = f\{\Delta\hat{s}_1(\tau+1), \ldots, \Delta\hat{s}_i(\tau+1), \ldots, \Delta\hat{s}_N(\tau+1)\}. \quad (8)$$

4. Идентификация параметров условной по наблюдениям ПРВ $\hat{W}(\vec{S}_j(\tau+1))$ значений частных

показателей качества СОСК с использованием оценок его моментов

$$\mathrm{M}\{\Delta\hat{s}_i(\tau+1)/y_{\Delta\hat{s}_i}(\tau+1)\};\ \|\mathrm{D}\|;$$

5. Определение оценочных значений *j*-го ЧПЭФ на (τ+1)-ом такте (шаге) функционирования СОСК:

$$P_{\text{вып }j}(\tau+1)[(\vec{S}_j(\tau+1)\le\vec{S}_j^{\text{тр}})]=\int_0^{\vec{S}_j^{\text{тр}}}\hat{W}(\vec{S}_j(\tau+1))\,d\,\vec{S}_j;\quad(9)$$

6. Определение оценочного значения ОПЭФ на (τ+1)-ом такте (шаге) функционирования СОСК в соответствии с выражением (5)

$$\hat{P}_{\text{вып тр}}(\tau+1)=f\{\hat{P}_{\text{вып }1}(\tau+1),\ \hat{P}_{\text{вып }2}(\tau+1),\dots \\ \dots,\hat{P}_{\text{вып }j}(\tau+1),\dots,\hat{P}_{\text{вып }J}(\tau+1)\}.\quad(10)$$

Переход от стационарных аналитических моделей показателей качества СОСК к марковским моделям позволил исследовать переходные процессы изменения качества функционирования подсистем анализа смыслового наполнения информационных объектов и СОСК в целом. Предложенная рекуррентная форма записи ЧПЭФ и ОПЭФ СОСК позволяет получать их оценку в реальном масштабе времени. Это позволяет существенно снижать длительность цикла управления системами такого класса [15–18].

V. Выводы

Представленный подход может быть использован для решения задач прямой динамической оценки эффективности функционирования подсистем анализа смыслового наполнения информационных объектов и СОСК в целом, для обоснования оперативно-технических требований к ним, оптимизации их структуры и алгоритмов функционирования в интересах обнаружения ВИ. Таким образом, в статье предложена математическая модель процесса смены состояний показателей качества СОСК на основе марковских цепей. Модель служит основой методики оценки эффективности СОСК для обнаружения ВИ с учетом устранения неопределенности смыслового наполнения информационных объектов и учитывает вероятностно-временной механизм изменения состояния процесса функционирования систем такого класса в динамике. Описана методика многокритериального (векторного) динамического оценивания эффективности таких ситем, основанная на анализе текущих отклонений значений показателей качества СОСК от требований к ним. Методика учитывает переходные процессы при введении управлений структурой и параметрами СОСК, структурой и средствами механизмов обнаружения ВИ, методами, параметрами и режимами их работы в условиях различного вида воздействий. Перспективными направлениями дальнейшего развития методологии оценки эффективности являются задачи разработки методов оптимального управления эффективностью систем такого класса. Предложенная методика, в силу своей «открытости» для различных показателей качества СОСК, может быть положена в основу векторного динамического анализа эффективности любых других сложных систем. Методика оценивания эффективности СОСК может быть реализована в интересах оперативных структур управления политикой борьбы с нежелательной, сомнительной и вредоносной информацией. Может быть полезна техническим и проектным органам, отвечающим за разработку СОСК – с целью анализа вклада в эффективность их функционирования новых технических принципов построения алгоритмов, средств и комплексов обнаружения и противодействия ВИ, а также может найти свое применение при разработке плана инвестиций в промышленно-экономической области, отвечающей за реализацию систем контроля сетевого контента.

Список литературы

[1] Kotenko I.V. Chechulin A.A. Komashinsky D.A. Categorisation of web pages for protection against inappropriate content in the Internet. // International Journal of Internet Protocol Technology (IJIPT), 2017. 10 (1), pp. 61-71.

[2] Kotenko I.V., Chechulin A.A. Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing (California: IEEE Computer Society), 2012. pp. 94-101.

[3] Yuksel S. Control of Stochastic Systems. // Queen's University Mathematics and Engineering. 2017. 167 p.

[4] Van Handel R. Stochastic Calculus, Filtering and Stochastic Control. / Springer, New York. 2007. 261 p.

[5] Pfleeger C.P., Pfleeger S.L. Security in Computing. New Jersey, USA. Prentice Hall. 2015. 944 p.

[6] Dorf R., Bishop R. Modern Control Systems, 10th Edition, Prentice Hall, 2014. 1111 p.

[7] Zecevic A.I., Siljak D.D. Control of Complex Systems. London, Springer Science Business Media, 2010. 221 p.

[8] Trivedi K.S. Probability and Statistics with Reliability, Queuing and Computer Science Applications: Edition 2. John Wiley & Sons, Inc., Hoboken, New Jersey. USA. 2016. 880 p.

[9] Shuvalov I.A., Semenchin E.A. Mathematical model of impact of threats on information system of processing of personal information. // Fundamental Research. №10, 2013. pp. 529-533

[10] Stamp M. Information Security Principles and Practice. San Jose State University. 2005. 381 p.

[11] Quarteroni A. Mathematical Models in Science and Engineering. // Notices of the AMS. Volume 56, Number 1. 2009. p. 9-19.

[12] Myers A. Complex System Reliability. Springer Science & Business Media. Luxembourg. 2010. 238 p.

[13] Walliman N. Research methods: the basics. Taylor & Francis. London, UK. 2011. 190 p.

[14] Oliver D.W., Kelliher T.P., Keegan J.G. Engineering Complex Systems With Models and Objects. McGraw-Hill Companies. New York, USA. 2007. 325 p.

[15] Parashchuk I.B. Decision Support at the Phase of Estimation of Telecommunication Network Functioning Efficiency. // IEEE/ICC2001 // St. Petersburg International Conference on Communications. SPb.: SPbGTU «LETI», 2001. pp. 2-6.

[16] Parashchuk I.B. Parametrization principles of states space of Telecommunications network in the framework of formulation of problem of optimal adaptive networking monitoring. // Modern Science: Development Tendencies. VII Extramunal International Science-Practical Conference. Part II. Krasnodar, 2014. pp. 142-144.

[17] Kotenko I.V., Parashchuk I.B. Synthesis of Controlled Parameters of Cyber-Physical-Social Systems for Monitoring of Security Incidents in Conditions of Uncertainty. // 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) / IOP Conf. Series: Journal of Physics: Conference Series (JPCS) Vol.1069, 2018. pp 1-6.

[18] Kotenko I.V., Parashchuk I.B., Omar T.K. Neuro-Fuzzy Models in Tasks of Intelligent Data Processing for Detection and Counteraction of Inappropriate, Dubious and Harmful Information. // II International Scientific and Practical Conference «Fuzzy Technologies in the Industry» (FTI 2018), Ulyanovsk, Russia. / CEUR Workshop Proceedings (CEUR-WS). Vol-2258**,** 2018; pp. 116-125.