Формализации анализа влияния интеллектуальных агентов мониторинга на качество функционирования комплексных систем защиты информации

Л. К. Птицына[1], Н. Н. Эль Сабаяр Шевченко[2]
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
[1] ptitsina_lk@inbox.ru, [2]nzs.vus@gmail.com

М. П. Белов
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
milesa58@mail.ru

А. В. Птицын
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
pticin@inbox.ru

***Аннотация*. Представлены определяющие ориентиры цифровой экономики. Показана значимость информационной безопасности в цифровой экономике. Обоснована востребованность интеллектуальных комплексных систем защиты информации. Рассмотрены причины использования интеллектуальных агентных технологий при обеспечении информационной безопасности. Описаны современные тенденции развития исследований агентных технологий по профилю защиты информации. Предложены формализации анализа влияния агентов на качество функционирования комплексных систем защиты информации. Определён математический аппарат предложенных формализаций.**

Ключевые слва: управление качеством; комплексная система защиты информации; мониторинг; интеллектуальный агент; моделирование; пространство состояний; показатели качества; аналитика; выбор средств управления

Интеграция и взаимопроникновение научно-исследовательских, научно-методических, научно-практических, научно-технологических, экономических, образовательных, социальных, культурных и других процессов и явлений, превращение их в единое целое является характерной чертой развития современного социума. Движущей силой подобного развития социума стало формирование глобального информационного пространства и образование цифровой экономики.

При цифровой экономике данные в цифровой форме относятся к ключевым факторам производства во всех сферах социально-экономической деятельности, от которых становятся зависимыми конкурентоспособность страны, качество жизни граждан, уровень экономического роста и национальный суверенитет. Информационная инфраструктура и информационная безопасность рассматриваются в качестве основных инфраструктурных компонентов цифровой экономики.

Информационная безопасность становится неотъемлемой составляющей необходимых условий для развития общества знаний, повышения благосостояния и качества жизни граждан посредством повышения доступности и качества товаров и услуг цифровой экономики, повышения степени информированности и цифровой грамотности, улучшения доступности и качества государственных услуг для граждан и их безопасности.

Высокая степень развиваемости цифровых платформ и технологий отображается в обилии многообразия информационных инфраструктур, задействованных в цифровой экономике, и в расширении масштабов неопределённостей, касающихся состояний сред, в которых осуществляется деятельность. При широком спектре многообразия информационных инфраструктур в условиях разного рода неопределённостей ключевые задачи информационной безопасности решаются с использованием интеллектуальных комплексных систем защиты информации и управления их качеством.

Интеллектуальное профилирование комплексных систем защиты информации осуществляется по полному вариативу современных направлений развития теории, технологий и практики искусственного интеллекта, предусматривающих как преодоление субъективизма и разного рода неопределённостей, так и управление качеством защищённости от возможных угроз.

При всём многообразии интеллектуального профилирования комплексных систем защиты информации на интеллектуальные агентные технологии возлагаются не только функциональные, но управляющие задачи, поскольку именно с этими технологиями связано интеллектуальное планирование действий, сопровождающих распределение задач и ресурсов, принятие решений по обнаружению, идентификации и парированию угроз защищённости информации, формирование безопасной среды и конфигурации ресурсов, необходимых для успешного решения задач предметного характера.

В связи с этим в контексте обеспечения информационной безопасности проводятся научные исследования интеллектуальных агентных технологий, учитывающие различные аспекты их применения в информационных инфраструктурах [1, 2, 3].

Значительное внимание уделяется исследованиям организации мониторинга информационной безопасности [4]. Для последующего погружения в выяснение эффективных математических и технических решений для информационной инфраструктуры, связанных с использованием агентных технологий, требуется проведение анализа влияния агентов мониторинга на качество функционирования комплексных систем защиты информации.

Известные формализации исследования эффективности применения агентных технологий в интеллектуальных комплексных системах защиты информации ограничиваются анализом лучевых топологических приемов интеграции с возможными разветвлениями и масштабированием при комплексировании средств защиты информации, оставляя без внимания кольцевые приемы, применяемые в современных реализациях [5, 6, 7, 8].

Предлагаемые формализации для анализа влияния агентов на качество функционирования комплексных систем защиты информации предназначаются для:

- расширения возможностей аналитического определения и оценивания показателей статистических профилей качества функционирования интеллектуальных комплексных систем защиты информации, взаимодействующих с агентами мониторинга согласно кольцевым приемам интеграции объединяемых средств. При этом рассматриваются ситуации формирования ложных тревог и ситуации формирования решений относительно обнаружения, идентификации и парирования угроз информационной безопасности;
- управления качеством функционирования интеллектуальных комплексных систем защиты информации с агентами мониторинга.

Предлагаемая и раскрываемая методика базируется на системе новых разработанных формализаций, среди которых:

- формализация аналитического определения статистических профилей процессов, соответствующих функционированию средств интеллектуальной комплексной системы защиты информации и агента мониторинга, интеграция которых описывается с применением кольцевых приемов;
- формализация перехода от статистических профилей процессов к матричному описанию процессов функционирования средств интеллектуальной комплексной системы защиты информации и агента мониторинга;
- формализация формирования обобщённого матричного описания процессов совместного функционирования средств интеллектуальной комплексной системы защиты информации и агента мониторинга согласно кольцевому приему их интеграции;
- формализация аналитического определения статистического профиля совместного функционирования средств интеллектуальной комплексной системы защиты информации и агента мониторинга согласно кольцевому приему их интеграции;
- формализация определения показателей влияния агента мониторинга на качество функционирования комплексных систем защиты информации.

При моделировании процессов, соответствующих функционированию интеллектуальной комплексной системы защиты информации и агента мониторинга, могут рассматриваться любые приёмы комплексирования средств, различные способы синхронизации выполняемых процедур обработки информации и принятия решений, а также варьируемые границы масштабирования.

Представляемые далее формализации раскрываются для случаев проявления возможных угроз.

Комплексная система защиты информации описывается $f_N(k_N)$, $k_N = 1,2,...,M_1$ плотностью распределения вероятностей k_N дискретного времени защиты информации.

Активный агент мониторинга характеризуется $f_{am}(k_{am})$, $k_{am} = 1,2,...,M_2$ плотностью распределения вероятностей k_{am} дискретного времени мониторинга.

Указанные характеристики удовлетворяют следующим условиям:

$$\sum_{k_N=1}^{M_1} f_N(k_N) = 1, \quad \sum_{k_{am}=1}^{M_2} f_{am}(k_{am}) = 1.$$

Представленные характеристики находятся согласно методикам и математическим процедурам, описанным соответственно в [9] и [10].

Согласно разработанной методике первоначально процессы функционирования средств интеллектуальной комплексной системы защиты информации и процессы

функционирования активного агента мониторинга описываются в виде диаграмм деятельности.

Представление каждого действия в диаграмме деятельности дополняется статистической характеристикой.

При нахождении плотностей $f_N(k_N)$ и $f_{am}(k_{am})$ проводятся преобразования построенных расширенных объектно-ориентированных моделей.

В результате перехода от статистического профиля функционирования средств интеллектуальной комплексной системы защиты информации к $\mathbf{P}_N$ матричному описанию образуется формализация следующего вида:

$$\mathbf{P}_N = \begin{bmatrix} 0 & f_N(M_1) & f_N(M_1-1) & f_N(M_1-2) & f_N(M_1-3) & \dots & f_N(1) \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Матрица $\mathbf{P}_N$ характеризуется размерностью $(M_1+1)\times(M_1+1)$.

В результате перехода от статистического профиля процесса функционирования активного агента мониторинга к $\mathbf{P}_{am}$ матричному описанию формируется следующее представление:

$$\mathbf{P}_{am} = \begin{bmatrix} 0 & f_{am}(M_2) & f_{am}(M_2-1) & f_{am}(M_2-2) & f_{am}(M_2-3) & \dots & f_{am}(1) \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Матрица $\mathbf{P}_{am}$ характеризуется размерностью $(M_2+1)\times(M_2+1)$.

Обобщённое $\mathbf{P}$ матричное описание процессов совместного функционирования средств интеллектуальной комплексной системы защиты информации и агента мониторинга согласно кольцевому приему их интеграции определяется следующим образом:

$$\mathbf{P} = \begin{bmatrix} 0 & f_N(M_1) & f_N(M_1-1) & f_N(M_1-2) & f_N(M_1-3) & \dots & f_N(1) & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & p & 0 & 0 & \dots & 0 & (1-p) \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & f_{am}(M_2) & f_{am}(M_2-1) & \dots & f_{am}(2) & f_{am}(1) \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}.$$

Приведённая квадратная матрица имеет размерность $(M_1+M_2+2)\times(M_1+M_2+2)$.

Плотность распределения вероятностей $k_{N,am}$ дискретного времени защиты информации при активном мониторинге $f_{N,am}(k_{N,am})$ находится согласно соотношению

$$f_{N,am}(k_{N,am}) = P_{1,(M_1+M_2+2)}^{(k_n,am)} - P_{1,(M_1+M_2+2)}^{(k_n,am-1)}$$

$$k_{N,am} = 1,2,\dots,K_{N,am},$$

где $P_{1,(M_1+M_2+2)}^{(k_n,am)}$ – $(1,(M_1+M_2+2))$-й элемент $k_{N,am}$ степени матрицы $\mathbf{P}$;

$P_{1,(M_1+M_2+2)}^{(k_n,am-1)}$ – $(1,(M_1+M_2+2))$-й элемент $(k_{N,am}-1)$ степени матрицы $\mathbf{P}$;

$K_{N,am}$ – верхняя граница дискретного времени $k_{N,am}$.

Значение $K_{N,am}$ определяется как наименьшее целое, удовлетворяющее условию

$$1-\sum_{k_{N,am}=1}^{K_{N,am}} (P_{1,(M_1+M_2+4)}^{(k_n,am)} - P_{1,(M_1+M_2+4)}^{(k_n,am-1)}) \le \delta,$$

где δ – сколь угодно малая величина.

Согласно теории марковских цепей для нахождения статистических характеристик дискретного времени защиты информации при совместном функционировании средств интеллектуальной комплексной системы и агента мониторинга согласно кольцевому приему их интеграции выполняются следующие матричные операции:

$$\mathbf{T} = (\mathbf{I} - \mathbf{P}_Q)^{-1},$$

$$\mathbf{t} = \mathbf{T}\mathbf{e},$$

$$\mathbf{D} = \mathbf{T}(2\mathbf{T}_0 - \mathbf{I}) - \mathbf{T}^*,$$

$$\mathbf{d} = (2\mathbf{T} - \mathbf{I})\mathbf{t} - \mathbf{t}^*,$$

где $\mathbf{I}$ – $(M_1+M_2+1)\times(M_1+M_2+1)$ – единичная матрица;

$\mathbf{P}_Q$ – $(M_1+M_2+1)\times(M_1+M_2+1)$ – матрица, получаемая из матрицы $\mathbf{P}$ посредством вычёркивания её последней строки и последнего столбца;

$\mathbf{T}$ – $(M_1+M_2+1)\times(M_1+M_2+1)$ – матрица, образованная элементами $T_{i,j}$ $i,j = 1,2,\dots,(M_1+M_2+1)$;

$T_{i,j}$ – математическое ожидание количества пребываний марковской цепи в j-ом состоянии, если за исходное принять i-ое состояние;

$\mathbf{e}$ – $(M_1+M_2+1)\times 1$ – единичный вектор-столбец;

$\mathbf{t}$ – $(M_1+M_2+1)\times 1$ – вектор-столбец, состоящий из элементов t_i;

t_i – среднее время, затрачиваемое на выполнение защиты информации при i-ом исходном состоянии;

$\mathbf{T}_0$ – $(M_1+M_2+1)\times(M_1+M_2+1)$ – матрица, получаемая из квадратной матрицы $\mathbf{T}$ заменой нулями всех элементов, не лежащих на главной диагонали;

$\mathbf{T}^*$ – матрица, получаемая из матрицы $\mathbf{T}$ возведением в квадрат каждого её элемента;

$\mathbf{D}$ – $(M_1+M_2+1)\times(M_1+M_2+1)$ – матрица, образованная элементами $D_{i,j}$ $i,j=1,2,...,(M_1+M_2+1)$;

$D_{i,j}$ – дисперсия количества пребываний марковской цепи в *j*-ом состоянии, если за исходное принять *i*-ое состояние;

$\mathbf{t}^*$ – вектор-столбец, получаемый из вектора $\mathbf{t}$ возведением в квадрат каждого его элемента;

$\mathbf{d}$ – $(M_1+M_2+1)\times 1$ – вектор-столбец, состоящий из элементов d_i;

d_i – дисперсия дискретного времени защиты информации при *i*-ом исходном состоянии.

Первый элемент вектора $\mathbf{t}$, а именно t_1, является математическим ожиданием дискретного времени защиты информации. Первый элемент вектора $\mathbf{d}$, а именно d_1, является дисперсией дискретного времени защиты информации. Наряду с нахождением точных значений статистических характеристик времени защиты информации предусматривается и вычисление их приближённых значений.

Приближённое оценивание $\mathrm{E}(k_{N,am})$ математического ожидания и $\mathrm{D}(k_{N,am})$ дисперсии дискретного времени защиты информации проводится с использованием плотности распределения вероятностей $k_{N,am}$ при активном мониторинге $f_{N,am}(k_{N,am})$. При этом вычисления осуществляются согласно следующим выражениям:

$$\mathrm{E}(k_{N,am}) \approx \sum_{k_{N,am}=1}^{K_{N,am}} k_{N,am} f_{N,am}(k_{N,am})$$

$$\mathrm{D}(k_{N,am}) \approx \sum_{k_{N,am}=1}^{K_{N,am}} (k_{N,am} - \mathrm{E}(k_{N,am}))^2 f_{N,am}(k_{N,am}).$$

Степень приближения к точным значениям может повышаться по мере уменьшения задаваемого значения величины δ.

Выведенные аналитические определения для оценивания t_1, d_1, $\mathrm{E}(k_{N,am})$, $\mathrm{D}(k_{N,am})$ вводятся в подсистему алгебраических инвариантов комплексной системы защиты информации с целью оперативного обнаружения возможных проявлений деструктивных воздействий.

В качестве алгебраических инвариантов определяются следующие соотношения:

$$t_1 - \mathrm{E}(k_{N,am}) < \varepsilon_1,$$

$$d_1 - \mathrm{D}(k_{N,am}) < \varepsilon_2,$$

где – ε_1, ε_2 задаваемые сколь угодно малые величины.

Подобным образом формируются формализации применительно к условиям отсутствия проявлений потенциально возможных угроз. В этом случае определяются статистические характеристики дискретного времени до ложного обнаружения проявления угроз.

Вслед за определением показателей статистических профилей качества функционирования интеллектуальной комплексной системы защиты информации, взаимодействующей с агентом мониторинга согласно кольцевому приёму интеграции объединяемых средств, выделяется параметрическое пространство, элементы которого оказывают существенное влияние на качество.

Сформированное параметрическое пространство и выведенные аналитические определения показателей статистических профилей информации являются математическим базисом для ситуационного управления качеством функционирования интеллектуальной комплексной системы защиты, взаимодействующей с агентом мониторинга согласно кольцевому приёму интеграции объединяемых средств.

Заключение

Разработанные формализации представляют собой расширения для ситуационного управления качеством интеллектуальных комплексных систем защиты информации.

Список литературы

[1] Котенко И.В., Уланов А.В. Агентно-ориентированное моделирование поведения сложных систем в среде Интернет // В сборнике: КИИ-2006. Десятая Национальная конференция по искусственному интеллекту с международным участием. Российская ассоциация искусственного интеллекта. 2006. С. 660-668.

[2] Уланов А.В., Котенко И.В. Система многоагентного моделирования механизмов защиты компьютерных сетей // В сборнике: КИИ-2006. Десятая Национальная конференция по искусственному интеллекту с международным участием. Российская ассоциация искусственного интеллекта. 2006. С. 867-876.

[3] Котенко И.В. Многоагентное моделирование для исследования механизмов защиты информации в сети Интернет // В сб.: имитационное моделирование. Теория и практика. Пленарные доклады. 2009. С. 38-47.

[4] Котенко И.В., Паращук И.Б. Автоматизированный адаптивный мониторинг комплексной безопасности информационных систем «умного города»: целевые функции концептуальной модели // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2018. № 3. С. 7-15.

[5] Птицын А.В. Формирование знаний по агентным технологиям информационной безопасности // Новые информационные технологии в образовании: Материалы X международной научно-практической конференции, Екатеринбург, 27 февраля–3 марта 2017 г. 2017. С. 92-94.

[6] Птицын А.В., Птицына Л.К. Обеспечение информационной безопасности на основе методологического базиса агентных технологий // Вестник Брянского государственного технического университета. № 2(55). 2017. С. 146-154.

[7] Птицын А.В., Лебедева А.А., Белов М.П., Птицына Л.К. Исследование реактивных действий информационного агента под влиянием инфокоммуникационной среды // Проблемы управления в технических системах. II Международная научная конференция: сб. науч. ст. СПб.: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», 2017. С. 21–24.

[8] Птицына Л.К., Лебедева А.А., Птицын А.В. Расширение знаний о качестве функционирования интеллектуальных информационных агентов // Новые информационные технологии в образовании: материалы XI междунар. науч.-практ. конф., Екатеринбург, 27 февраля– 3 марта 2018 г., ФГ АОУ ВО «Рос. гос. проф.-пед. ун-т». Екатеринбург, 2018. С. 577-583.

[9] Птицына Л.К. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL: учеб. пособие / Л.К. Птицына, Н.Г. Смирнов. СПб.: Изд-во Политехн. ун-та, 2011. 105 с.

[10] Птицын А.В., Птицына Л.К. Аналитическое моделирование комплексных систем защиты информации. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 293 с.