Методика контроля и восстановления целостности вычислительных процессов в информационных системах на основе приобретаемого кибериммунитета

Балябин Артём Алексеевич
ведущий инженер-программист, АО «Технологии радиоконтроля», г. Санкт-Петербург, Россия, treven.wt@yandex.ru

АННОТАЦИЯ

Введение: в работе предложена методика автоматизированного контроля и восстановления целостности вычислительных процессов в информационных системах на основе приобретаемого кибериммунитета. **Постановка задачи:** разработка методики автоматизированного контроля и восстановления целостности вычислительных процессов, позволяющей осуществлять динамический контроль вычислений, выявлять их искажения, восстанавливать корректное состояние вычислительных процессов и накапливать знания об искажениях для повышения эффективности восстановления в будущем. **Методы:** методы теории вычислительных процессов; методы теории подобия и размерностей; модели и методы теории надежности. **Результаты:** разработана методика контроля и восстановления целостности вычислительных процессов в информационных системах, позволяющая на основе положений теории подобия и размерностей формировать цифровой паспорт вычислительного процесса в терминах размерностей, осуществлять динамический контроль целостности вычислительных процессов, выявлять признаки наличия нарушений целостности вычислений, осуществлять их восстановление, а также осуществлять самообучение и накопление новых знаний приобретаемого кибериммунитета. **Практическая значимость:** предложенная методика контроля и восстановления целостности вычислительных процессов на основе приобретаемого кибериммунитета позволяет выявлять аномалии функционирования информационных систем, возникшие в результате вредоносных воздействий, противодействовать им, восстанавливать параметры поведения системы, а также осуществлять накопление новых знаний кибериммунитета о вредоносных воздействиях для повышения эффективности противодействия кибератакам в будущем. **Обсуждение:** новизна предложенной методики состоит в наличии способности накапливать «иммунную память», планировать процедуру «иммунного ответа» и осуществлять самовосстановление в реальном масштабе времени, что позволяет противодействовать уже встречавшимся и вновь появляющимся кибератакам.

КЛЮЧЕВЫЕ СЛОВА: вычислительный процесс; информационная система; киберустойчивость; приобретаемый кибериммунитет; самовосстановление.

Введение

В условиях роста угроз безопасности, увеличения количества и сложности кибератак, становится ощутимой недостаточная эффективность существующих методов и средств защиты информации. Сложный, многоуровневый характер организации современных информационных систем снижает их прозрачность и затрудняет интеллектуальное управление и обеспечение их безопасности [1].

Применяемые сегодня подходы к обеспечению отказоустойчивости и надежности в большинстве случаев сводятся к внедрению элементов структурно-функциональной избыточности, обеспечивающих реконфигурацию, эталонирование, репликацию, возврат к контрольным точкам и др. На сегодняшний день они не способны в полной мере предотвратить возможные серьезные последствия от реализации угроз безопасности, а методы, сводящиеся к восстановлению из контрольных точек и рестарту вычислительных процессов, могут приводить к длительному простою или недоступности системы, а также частичной или полной потере обрабатываемой информации, что недопустимо для систем с высокими требованиями к надежности и отказоустойчивости. Кроме этого, ландшафт угроз постоянно меняется: выявляются новые уязвимости программного и аппаратного обеспечения, применяются более сложные техники и тактики нападения, совершенствуются способы обхода средств защиты. Более 40% кибератак используют новые уязвимости и способы обхода систем защиты, и не обнаруживаются существующими системами обнаружения вторжений, системами противодействия компьютерным атакам и иными средствами защиты [1]. Актуальность данной работы обуславливается необходимостью обеспечения киберустойчивости информационных систем в условиях роста угроз безопасности, а также наделения их способностью противодействовать как известным, так и ранее неизвестным кибератакам.

Степень разработанности темы

Проблема восстановления корректности функционирования информационных систем в условиях вредоносных воздействий и связанные с ней являются предметом изучения отечественных и зарубежных исследователей.

В работах [1-8] рассматриваются возможные решения научно-технической проблемы придания информационным системам свойств, позволяющих предотвратить катастрофические последствия от реализации кибератак злоумышленников. Большое внимание уделено развитию идей кибериммунитета, в частности, изучению и формализации закономерностей его формирования, накопления и применения.

Работы [9, 10] посвящены анализу биологических метафор и подходов, применимых для защиты компьютерных систем, таких как нейронные сети, эволюционные методы, иммунные системы и др., а также предлагаются варианты их комплексирования. В работе [10] представлена система обнаружения атак, использующая в своей работе методы машинного обучения и технологии обработки больших данных. Общим для систем подобного типа является то, что для обнаружения воздействий используются в основном сигнатурные и корреляционные методы, которые обладают высокой точностью при выявлении уже известных или слабо отклоняющихся от известных воздействий. Однако, для выявления и своевременного реагирования на ранее неизвестные кибератаки требуется применение иных методов – инвариантных.

Задача выделения признаков поведения программ защищаемой информационной системы (корректное или некорректное поведение), инвариантных относительно условий их функционирования, эквивалентна задаче определения изоморфности двух систем относительно заданного отображения. Математический аппарат теории подобия и размерностей может применяться для установления необходимых и достаточных условий изоморфности таких систем, а также для определения качественных и количественных параметров изоморфизма. Основные положения теории подобия формулировались в работах А. А. Гухмана, М. В. Кирпичева, В. А. Веникова, Л. И. Седова применительно к процессам, происходящим в электрических и механических системах. Позднее теория подобия и размерностей была применена и для моделирования вычислительных процессов, в частности, и в области кибербезопасности. Так в работах [11-16] рассматриваются вопросы, связанные со статической и динамической верификацией вычислительных программ на основе инвариантных соотношений подобия, в частности, предлагается осуществлять формирование цифрового паспорта, включающего в себя инварианты подобия, характеризующие расчетные алгоритмы программы, и производить динамический контроль корректности вычислений путем построения аналогичных инвариантов в условиях воздействий и сравнения их с эталонными. Предложенные способы позволяют выявлять нарушения целостности вычислений, вызванные в том числе и ранее неизвестными воздействиями, однако, вопросы, связанные с автоматизацией построения цифрового паспорта и накоплением информации о выявленных нарушениях целостности вычислений, в работах не рассматривались.

Работа [17] посвящена разработке методов и средств обеспечения устойчивости функционирования программ в условиях вредоносных воздействий. Авторы предлагают метод контроля корректности вычислительных процессов на основе временных автоматов, использующих эталонные профили, являющиеся инвариантами относительно обрабатываемых данных и маршрутов выполнения программ. Стоит отметить, что такой метод позволяет контролировать лишь корректность переходов между линейными участками программы и время их выполнения, что не гарантирует корректность вычислений внутри этих линейных участков.

Работы [18-20] посвящены развитию идей, изложенных в [1-8, 11-16]. В работе [18] предложен алгоритм паспортизации программ, а в работах [19, 20] – алгоритмы обнаружения аномалий на основе теории подобия и размерностей, позволяющие осуществлять контроль семантической корректности вычислений и гарантировать корректность их результатов.

Ввиду постоянного роста сложности программного и аппаратного обеспечения информационных систем очевидна неизбежность появления новых уязвимостей и способов их эксплуатации. С другой стороны, существует необходимость обеспечения требуемой устойчивости и надежности информационных систем. С учетом данного противоречия можно сделать вывод об актуальности задачи исследования возможностей организации систем защиты на основе биоинспирированных подходов, в частности, на основе свойств иммунитета живого организма, для противодействия как известным, так и ранее неизвестным кибератакам, и упреждения их последствий. Принципиальным отличием данного подхода от уже существующих является наличие способности систем защиты адаптироваться и накапливать «иммунную память» к известным и новым кибератакам, планировать и осуществлять самовосстановление в реальном масштабе времени.

Для разрешения обозначенного противоречия в данной работе предложена методика автоматизированного контроля и восстановления целостности вычислительных процессов, сущность которой заключается во внедрении в исполняемый код программы элементов структурно-функциональной избыточности с последующим их контролем и восстановлением в случае обнаружения искажений.

Модель вычислительного процесса в условиях воздействий

Рассмотрим два вычислительных процесса p_1 и p_2, представимых уравнениями, имеющими вид [15]:

$$\sum_{i=1}^{q} \varphi_{ui} = 0, u = 1,2,...,r ;$$

$$\sum_{i=1}^{q} \phi_{ui} = 0, u = 1,2,...,r ;$$

где $\varphi_u = \prod_{j=1}^{n} x_j^{\alpha_{ul}}$ и $\phi_u = \prod_{j=1}^{n} X_j^{\alpha_{ul}}$ – однородные функции, зависящие от входных параметров вычислительных процессов.

В соответствии с прямой теоремой подобия, если процессы однородно подобны, то справедлива система:

$$\frac{\varphi_{ui}}{\varphi_{uq}} = \frac{\phi_{ui}}{\phi_{uq}}, u = 1,2,...,r; s = 1,2,...,(q-1).$$

Здесь выражения вида:

$$\pi_{us} = \frac{\varphi_{ui}}{\varphi_{uq}},$$

описывают так называемые критерии подобия (инварианты), которые, в соответствии с теоремой подобия, численно равны для взаимно подобных вычислительных процессов. Таким образом равенство критериев подобия является необходимым условием отнесения вычислительных процессов к подклассу взаимно подобных. Обратная теорема подобия формулирует достаточные условия и гласит, что два процесса однородно подобны, если их полные уравнения возможно привести к виду, в котором инварианты подобия численно равны [1].

Представим вычислительный процесс P в виде [15]:

$$P = < T, X, Y, Z, F, \Phi > ,$$

где T – моменты времени t, в которые осуществляется наблюдение за вычислительным процессом;

X – множество входных параметров вычислительного процесса;

Y – множества выходных параметров вычислительного процесса;

Z – множество $Z_{kj}(j = \overline{1,m})$ состояний вычислительного процесса, характеризующихся в каждый момент времени $t \in T$ выполняемыми в определенной последовательности в контрольной точке k арифметическими операциями;

F – множество операторов перехода f_i, отвечающих за изменение состояния вычислительного процесса;

Ф – множество операторов выхода ϕ_i, отвечающих за формирование результатов вычислений.

Для определения отношений между описанными множествами введем отображения:

$\lambda : T \times X \to Z'$ – отображение, действующее из множества входных параметров вычислительного процесса X, определяемых в моменты времени T, в множество состояний вычислительного процесса Z', и определяющее воздействия на вычислительный процесс;

$\psi : Z' \to \Pi'$ – отображение, действующее из множества состояний вычислительного процесса Z' в множество инвариантов подобия П', определяющее формирование инвариантов подобия в условиях воздействий;

$\mu : \Pi' \to \Pi$ – отображение, действующее из множества инвариантов подобия в условиях воздействий П' в множество эталонных инвариантов П, определяющее сравнение их между собой;

$\upsilon : \Pi \to E$ – отображение, действующее из множества инвариантов подобия П в множество ошибок E, определяющее сигнал о нарушении целостности вычислений;

$\xi : \Pi \to Z$ – отображение, действующее из множества инвариантов подобия П в множество состояний вычислительного процесса Z, определяющее восстановление вычислений;

$\chi : Z \to Y$ – отображение, действующее из множества состояний Z в множество выходных параметров вычислительного процесса Y, определяющее вычисление корректного результата.

Тогда процесс вычислений с учетом внешних воздействий, обнаружения аномалий и восстановления можно представить как показано на рисунке 1.

Рис. 1. Общий вид диаграммы отображений вычислительного процесса с восстановлением

Для контроля семантической корректности вычислительного процесса необходимо строить граф потока управления (ГПУ) программы [15]:

$$\Gamma(B, D),$$

где $B = \{B_i\}$ – множество линейных участков программы (вершины ГПУ);

$D = \{B \times B\}$ – множество связей по управлению между линейными участками (дуги ГПУ).

Каждый линейный участок $B_i \in B$ ГПУ характеризуется определенной последовательностью арифметических операторов:

$$B_i = (b_{i1}, b_{i2}, ..., b_{il}).$$

Каждому элементарному пути в ГПУ соответствует упорядоченная последовательность выполняемых линейных участков:

$$B^k = \left(B_1^k, B_2^k, ..., B_t^k\right),$$

где $B^k \subseteq B$ и $B_i^k = \left(b_{i1}^k, b_{i2}^k, ..., b_{il}^k\right), \forall i = \overline{1, p}$ есть последовательность арифметических операторов, выполняемых на линейном участке программы – реализация или вычислительный процесс, – которая является фрагментом программы, потенциально подверженным вредоносным воздействиям в виде искажения арифметических операторов.

Представление алгоритма вычислительного процесса в виде ГПУ необходимо для того, чтобы все арифметические операторы оказались внутри линейных участков и не были связаны с операторами переходов между ними. Это позволяет внедрить контрольные точки с целью расчета соотношений подобия для каждого линейного участка и определения пути в ГПУ. Таким образом достигается не только контроль целостности потока управления, но и контроль целостности вычислений на линейных участках [1].

Применение теории подобия и размерностей для контроля целостности вычислительных процессов

Исследования, проведенные в работе [1], показали, что проверка соотношений, опирающихся на свойства вычислений, является наиболее эффективным способом контроля корректности вычислений, поскольку они задают семантические связи между объектами программы, вычислимы в динамике ее выполнения, и, кроме того, инвариантны относительно входных данных и путей выполнения программы. Однако, задача вычисления инвариантов подобия на основе различных представлений программ является слабо поддающейся формализации.

Обозначим за $f_i^k\left(x_1, x_2, ..., x_N\right)$ первичное соотношение, соответствующее группе арифметических операторов. Тогда для *k*-ой реализации УГП B^k возможно записать последовательность первичных соотношений в виде [15]:

$$\begin{cases} y_1 = f_1^k\left(x_1, x_2, ..., x_N\right), \\ y_2 = f_2^k\left(x_1, x_2, ..., x_N, y_1\right), \\ ... \\ y_M = f_M^k\left(x_1, x_2, ..., x_N, y_1, y_2, ..., y_{M-1}\right). \end{cases}$$

Выполним суперпозицию $\{y_i\}$ в правых частях выражений и получим систему соотношений, инвариантных относительно перестановок:

$$\begin{cases} y_1 = z_1^k\left(x_1, x_2, ..., x_N\right), \\ y_2 = z_2^k\left(x_1, x_2, ..., x_N\right), \\ ... \\ y_m = z_m^k\left(x_1, x_2, ..., x_N\right). \end{cases} \quad (1)$$

Каждое *i*-ое соотношение $y_i = z_i^k\left(x_1, x_2, ..., x_N\right)$ можно представить в виде суммы степенных одночленов:

$$y_i = \sum_{i=1}^{p_i} z_{ij}\left(x_1, x_2, ..., x_N\right),$$

где $z_{ij}\left(x_1, x_2, ..., x_N\right)$ – степенной одночлен.

Слагаемые суммы (1) должны иметь одинаковые размерности, то есть должно выполняться равенство:

$$\left[y_i\right] = \left[z_{ij}\left(x_1, x_2, ..., x_N\right)\right],\ j = \overline{1, p_i}$$

или

$$\left[z_{ij}\left(x_1, x_2, ..., x_N\right)\right] = \left[z_{il}\left(x_1, x_2, ..., x_N\right)\right],\ j, l = \overline{1, p_i}\ . \quad (2)$$

Система (2) называется системой определяющих соотношений.

Зададим функцию $\rho = X \to \left[X\right]$, которая каждому $x_j \in X$ ставит в соответствие его абстрактную размерность $\left[x_j\right] \in \left[X\right]$. Тогда размерности в выражении (2) выразятся как:

$$\left[z_{ij}\left(x_1, x_2, ..., x_N\right)\right] = \prod_{n=1}^{N}\left[x_n\right]^{\lambda_{jn}},\ j = \overline{1, p_i}\ .$$

Используя (1) и (2), построим систему соотношений:

$$\prod_{n=1}^{N}\left[x_n\right]^{\lambda_{jn}} = \prod_{n=1}^{N}\left[x_n\right]^{\lambda_{ln}},\ j, l = \overline{1, p_i}\ ,$$

или:

$$\prod_{n=1}^{N}\left[x_n\right]^{\lambda_{jn} - \lambda_{ln}} = 1,\ j, l = \overline{1, p_i}\ . \quad (3)$$

Логарифмируя выражения системы (3), получим систему линейных однородных уравнений, называемую критерием семантической корректности:

$$\sum_{n=1}^{N}\left(\lambda_{jn} - \lambda_{ln}\right)\ln\left[x_n\right] = 0,\ j, l = \overline{1, p_i}\ . \quad (4)$$

Выполнив подобное (4) преобразование для $\forall B_i^k \in B^k$, получим систему однородных уравнений *k*-ой реализации вычислительного процесса [15]:

$$A^k \omega = 0\ .$$

Для формирования цифрового паспорта программы необходимо учитывать различные возможные реализации вычислительных процессов. В общем случае программа представляется совокупностью взаимосвязанных функциональных модулей, предназначенных для ре-

шения определенной задачи. Каждая отдельная реализация $B_i^k \in B^k$ является частным решением такой задачи, соответствующим последовательности арифметических операций при входных данных X. Поскольку последовательности арифметических операций, соответствующие различным реализациям могут частично совпадать, то есть $B^k \cap B^l \neq \varnothing, \forall B^k, B^l \in B$, то математические зависимости между группами арифметических операторов при переходе между этими реализациями также должны сохраняться, что позволяет говорить об общности критериев подобия [1]. Исходя из этого, q матриц $\{A^k\}$, соответствующих реализациям $\{B^k\}$, возможно объединить в систему:

$$A = \begin{pmatrix} A_1 \\ \dots \\ A_q \end{pmatrix}.$$

Такая система представляет собой базу данных эталонных инвариантов для линейных участков программы и является частью ее паспорта. При анализе исполняемого файла инварианты внедряются в него в качестве контрольных точек с целью последующего контроля размерностей в процессе выполнения программы. В каждой контрольной точке управление передается библиотеке паспорта для расчета фактических семантических инвариантов и сравнения их с эталонными. Если полученные инварианты совпадают, управление возвращается выполняемой программе, иначе формируется сигнал нарушения целостности вычислений, после чего осуществляется выработка плана восстановления и запоминание обнаруженного нарушения. На рисунке 2 представлена схема механизма контроля паспортизированного вычислительного процесса [19].

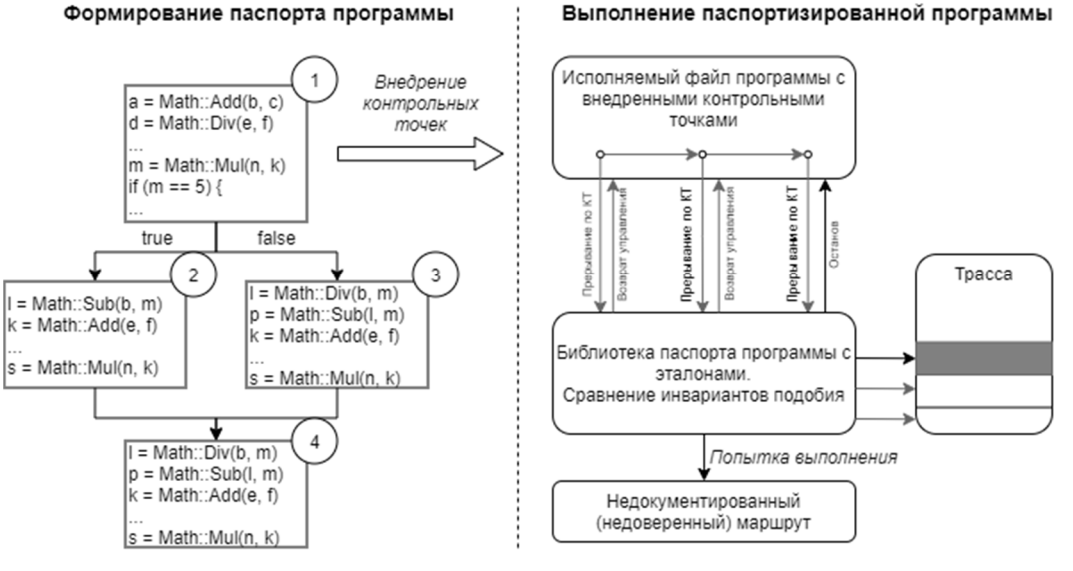

Рис. 2. Механизм контроля паспортизированного вычислительного процесса

Методика контроля и восстановления целостности вычислительных процессов

Общая схема методики приведена на рисунке 3.

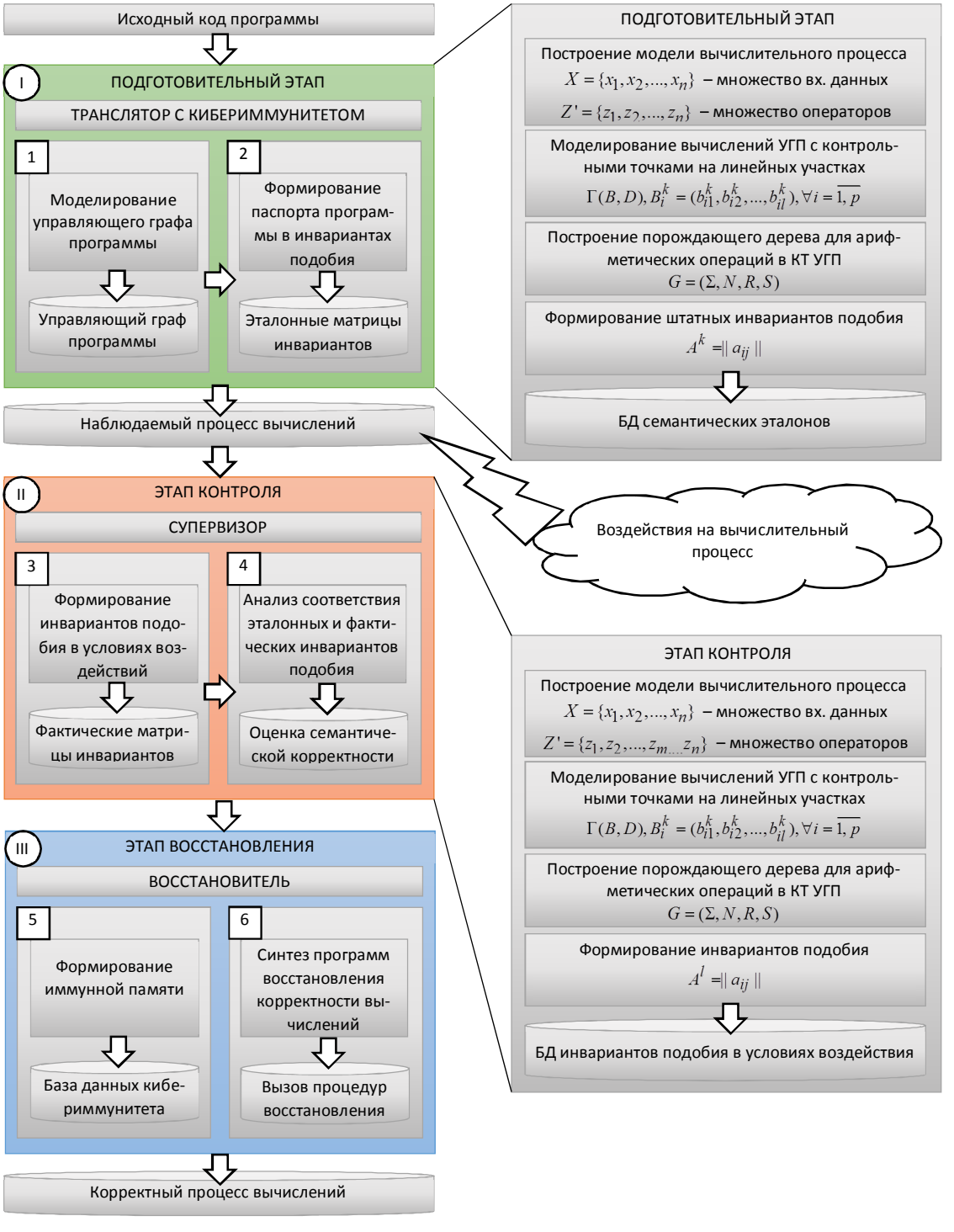

Рис. 3. Общая схема методики контроля и восстановления корректности вычислений

На этапе трансляции (компиляции) в исполняемый код программы встраиваются контрольные точки, сформированные на основе соотношений, сформулированных в терминах теории подобия, предназначенные для контроля семантической целостности вычислений на критических участках программы. Информация об эталонных соотношениях подобия (инвариантах), а также допустимых маршрутах выполнения программы составляет ее цифровой паспорт. В процессе функционирования кибериммунной системы защиты и противодействия выявляемым кибератакам в системе формируется информация об их типах и характеристиках. Для накопления такой информации с целью повышения оперативности реагирования кибериммунной системы защиты на угрозы данного типа в будущем, в ней существует подсистема хранения новых знаний кибериммунитета. При обнаружении искажения вычислений (отклонения потока управления от допустимых декларированных маршрутов, подмены вычислительных операторов и др.), осуществляется классификация характера нарушения и поиск его источника. В случае, если информация об обнаруженном воздействии отсутствует в базе данных кибериммунитета, запускается процедура самообучения и формирования новых знаний о выявленных нарушениях, после чего осуществляется синтез микропрограмм и запускается процедура восстановления, сводящаяся к точечным воздействиям, направленным на возврат вычислительного процесса в корректное состояние. Точечное воздействие позволяет восстановить искаженные вычисления без необходимости перезапуска вычислительного процесса, что минимизирует риски потери обрабатываемой информации и повышает оперативность восстановления.

Заключение

Предложенная в работе методика контроля и восстановления целостности вычислительных процессов на основе приобретаемого кибериммунитета позволяет выявлять аномалии функционирования информационных систем, возникшие в результате вредоносных воздействий (в том числе и ранее неизвестных), заключающиеся в искажении вычислений, противодействовать им, осуществлять восстановление параметров поведения системы, влияющих на ее киберустойчивость, а также осуществлять накопление знаний о воздействиях для повышения эффективности противодействия кибератакам в будущем.

Литература

1. *Петренко С. А.* Кибериммунология: научная монография / Петренко С. А. СПб: «Издательский Дом «Афина», 2021. 240 с.

2. *Petrenko S.* Cyber Resilience / S. Petrenko. Denmark (Gistrup): River Publishers, 2019. – 444 p.

3. *Петренко С. А.*, *Ступин Д. Д.* Национальная система раннего предупреждения о компьютерном нападении. 2-е издание. СПб: Издательский Дом "Афина", 2018. 448 с.

4. *Петренко С. А*. Обзор методов иммунной защиты Индустрии 4.0 // Защита информации. Инсайд. 2019. № 5(89). С. 36-48.

5. *Petrenko S*. Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation. Cham, Switzerland: Springer International Publishing, 2018. 249 p. DOI: 10.1007/978-3-319-79036-7.

6. *Petrenko S.* Cyber resilient platform for Internet of things (IIOT/IOT)ed systems: survey of architecture patterns // Voprosy Kiberbezopasnosti. 2021. № 2(42). P. 81-91. DOI: 10.21681/2311-3456-2021-2-81-91.

7. *Petrenko A. S.*, *Petrenko S. A.*, *Makoveichuk K. A.*, *Chetyrbok P. V.* Protection model of PCS of subway from attacks type «wanna cry», «petya» and «bad rabbit» IoT, 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2018. P. 945–949. DOI: 10.1109/EIConRus.2018.8317245.

8. *Petrenko S. A.*, *Stupin D. D.* Analytical Verification of Computational Programs. 2018 Engineering and Telecommunication (EnT-MIPT), IEEE, 2018, Moscow, Russia, pp. 127–129. DOI: 10.1109/EnT-MIPT.2018.00046.

9. *Клеверов Д. А.*, *Котенко И. В.* Адаптация биоинспирированных алгоритмов обнаружения кибератак для анализа больших объемов сетевого трафика // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020) : IX Международная научно-техническая и научно-методическая конференция : сборник научных статей, Санкт-Петербург, 26–27 февраля 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020. С. 583-588.

10. *Браницкий, А. А.* Архитектура сетевой системы обнаружения атак на основе использования методов машинного обучения и технологий обработки больших данных // Инновации в информационных технологиях, машиностроении и автотранспорте (ИИТМА-2020) : сборник материалов IV Международной научно-практической конференции с онлайн-участием, Кемерово, 07–10 декабря 2020 года. – Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2020. С. 160-162.

11. *Петренко А. А.*, *Маковейчук К. А.*, *Петренко С. А.* Программно-определяемая система хранения данных на основе теории подобия и размерностей // Информационные системы и технологии в моделировании и управлении : Сборник трудов V Международной научно-практической конференции, Ялта, 20–22 мая 2020 года / Отв. редактор К.А. Маковейчук. – Ялта: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2020. С. 220-224.

12. *Петренко С. А.* Киберустойчивость индустрии 4.0 / С. А. Петренко. СПб: Издательский Дом "Афина", 2020. 256 с.

13. *Петренко С. А.*, *Костюков А. Д.* Методика гибридного мониторинга угроз безопасности // Защита информации. Инсайд. 2020. № 2(92). С. 4-16.

14. *Petrenko S.* Self-healing cloud computing // Voprosy Kiberbezopasnosti. 2021. № 1(41). P. 80-89. DOI: 10.21681/2311-3456-2021-1-80-89.

15. *Харжевская А. В.*, *Ломако А. Г.*, *Петренко С. А.* Представление программ инвариантами подобия для контроля искажения вычислений // Вопросы кибербезопасности. 2017. № 2(20). С. 9-20. DOI: 10.21581/2311-3456-2017-2-9-20.

16. *Воробьев Е. Г.*, *Петренко С. А.*, *Олаоде Дж. А.*, *Альшанская Т. В.* Методика самовосстановления вычислений в условиях возмущений // Материалы Международной конференции по мягким вычислениям и измерениям. Санкт-Петербург, 2018. Т. 1. С. 298-299.

17. *Мирзабаев А. Н.*, *Самонов А. В.* Метод обеспечения устойчивости вычислительного процесса в условиях воздействия вредоносных программ // Вопросы кибербезопасности. 2022. № 2(48). С. 63-71. DOI 10.21681/2311-3456-2022-2-63-71.

18. *Балябин А. А.*, *Петренко С. А.*, *Якимовская Р. Н.* Алгоритм паспортизации вычислений SAP HANA на основе размерностей // Повышение конкурентоспособности социально-экономических систем в условиях трансграничного сотрудничества регионов : Сборник материалов IX международной научно-практической конференции, Ялта, 05–08 апреля 2022 года / Отв. редактор А.В. Олифиров. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2022. С. 68-71.

19. *Балябин А. А.*, *Петренко С. А.*, *Антонов В. В.* Алгоритм обнаружения аномалий функционирования SAP HANA на основе размерностей // Повышение конкурентоспособности социально-экономических систем в условиях трансграничного сотрудничества регионов : Сборник материалов IX международной научно-практической конференции, Ялта, 05–08

апреля 2022 года / Отв. редактор А.В. Олифиров. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2022. С. 61-64.

20. *Балябин А. А.*, *Петренко С. А.*, *Голумбовская А. Н.* Алгоритм выявления аномалий функционирования системных приложений в условиях отсутствия исходных кодов // Повышение конкурентоспособности социально-экономических систем в условиях трансграничного сотрудничества регионов : Сборник материалов IX международной научно-практической конференции, Ялта, 05–08 апреля 2022 года / Отв. редактор А.В. Олифиров. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2022. С. 65-68.

METHODOLOGY FOR MONITORING AND RESTORING THE INTEGRITY OF COMPUTING PROCESSES IN INFORMATION SYSTEMS BASED ON ACQUIRED CYBER IMMUNITY

ARTYOM A. BALYABIN
Senior Software Engineer, AO "Radiomonitoring Technology"
St. Petersburg, Russia, treven.wt@yandex.ru

ABSTRACT

Introduction: the paper proposes a technique for automated control and restoring of the integrity of computing processes in information systems based on acquired cyber immunity. **Problem statement:** development of a methodology for automated control and restoring of the integrity of computing processes, which allows to control the calculations dynamically, to detect their distortions, to restore the correct state of computing processes and to accumulate knowledge about distortions to improve recovery efficiency in the future. **Methods:** methods of the theory of computational processes; methods of the theory of similarity and dimensions; models and methods of reliability theory. **Results:** a technique for monitoring and restoring the integrity of computing processes in information systems based on the provisions of the theory of similarity and dimensions has been developed. It allows to form a digital passport of the computing process in terms of dimensions, to dynamically monitor the integrity of computing processes, to identify signs of violations of the integrity of calculations, to restore them, and also to carry out self-learning and accumulation of new knowledge of the acquired cyber immunity. **Practical relevance:** the proposed method for monitoring and restoring the integrity of computing processes based on acquired cyber immunity makes it possible to detect anomalies in the behavior of systems that have arisen as a result of destructive influences (including previously unknown ones), to counteract them, to carry out self-restoring of behavioral parameters that affect the cyber stability of the system, and also accumulate knowledge about the impacts to improve the efficiency of the implementation of the "cyber immune response" to invasions in the future. **Discussion:** the novelty of the proposed technique lies in the ability to accumulate "immune memory", plan the "immune response" procedure and carry out self-restoring in real time, which makes it possible to counteract known and yet unknown cyberattacks.

Keywords: computing process; information system; cyber resilience; acquired cyber immunity; self-restoring.

REFERENCES

1. Petrenko S. A. Kiberimmunologiya: nauchnaya monografiya / Petrenko S. A. [Cyber Immunology. The scientific monograph]. Saint-Petersburg: Izdatel'skiy Dom «Afina», 2021. 240 p. (In Rus).
2. Petrenko S. Cyber Resilience / S. Petrenko. Denmark (Gistrup): River Publishers, 2019. – 444 p.
3. Petrenko S. A., Stupin D. D. Nacional'naja sistema rannego preduprezhdenija o komp'juternom napadenii / 2-e izdanie [National system of advance computer attacks alerting]. Saint-Pertersburg: Izdatel'skiy Dom «Afina», 2018. 448 p. (In Rus).
4. Petrenko S. A. Industry 4.0 immune defence review. Zashhita informacii. Insajd [Zaŝita informacii. Inside]. 2019. № 5(89). Pp. 36-48. (In Rus).
5. Petrenko S. Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation. Cham, Switzerland: Springer International Publishing, 2018. 249 p. DOI: 10.1007/978-3-319-79036-7.
6. Petrenko S. Cyber resilient platform for Internet of things (IIOT/IOT)ed systems: survey of architecture patterns // Voprosy Kiberbezopasnosti. 2021. No 2(42). P. 81-91. DOI: 10.21681/2311-3456-2021-2-81-91.
7. Petrenko A. S., Petrenko S. A., Makoveichuk K. A., Chetyrbok P. V. Protection model of PCS of subway from attacks type «wanna cry», «petya» and «bad rabbit» IoT, 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). 2018. P. 945–949. DOI: 10.1109/EIConRus.2018.8317245.
8. Petrenko S. A., Stupin D. D. Analytical Verification of Computational Programs. 2018 Engineering and Telecommunication (EnT-MIPT), IEEE, 2018, Moscow, Russia, pp. 127–129. DOI: 10.1109/EnT-MIPT.2018.00046.
9. Kleverov D. A., Kotenko I. V. Adaptatsiya bioinspirirovannykh algoritmov obnaruzheniya kiberatak dlya analiza bol'shikh ob"emov setevogo trafika [Adaptation of bio-inspired algorithms for computer security analysis to big data technologies]. Materialy IX Mezhdunarodnoy nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii «Aktual'nye problemy infotelekommunikatsiy v nauke i obrazovanii» [Proceedings of the IX International scientific-technical and scientific-methodical conference «Actual problems of infotelecommunications in science and education», Saint-Petersburg, on February 26-27, 2020]. Saint-Petersburg, 2020. Pp. 583-588. (In Rus).
10. Branitskiy A. A. Arkhitektura setevoy sistemy obnaruzheniya atak na osnove ispol'zovaniya metodov mashinnogo obucheniya i tekhnologiy obrabotki bol'shikh dannykh [Architecture of a network attack detection system based on the usage of machine learning methods and big data processing technologies]. Materialy IV Mezhdunarodnoy nauchno-prakticheskoy konferentsii s onlayn-uchastiem «Innovatsii v informatsionnykh tekhnologiyakh, mashinostroenii i avtotransporte» [Proceedings of the IV International scientific-practical conference with online participation «Innovations in information technology, mechanical engineering and motor transport», Kemerovo, on December 07-10, 2020]. Kemerovo, 2020. Pp. 160-162. (In Rus).
11. Petrenko A. A., Makoveichuk K. A., Petrenko S. A. Programmno-opredelyaemaya sistema khraneniya dannykh na osnove teorii podobiya i razmernostey [Software-defined data storage system based on the theory of similarity and dimensions]. Materialy V Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnye sistemy i tekhnologii v modelirovanii i upravlenii» [Proceedings of the V International scientific-practical conference «Information systems and technologies in modeling and management», Yalta, on May 20-22, 2020]. Yalta, 2020. Pp. 220-224. (In Rus).
12. Petrenko S. A. Kiberustoychivost' industrii 4.0 [Cyber resilience industry 4.0]. Saint-Petersburg: Izdatel'skiy Dom «Afina», 2020. 256 p. (In Rus).
13. Petrenko S. A., Kostyukov A. D. Hybrid security threat monitoring. Zashhita informacii. Insajd [Zaŝita informacii. Inside]. 2020. № 2(92). Pp. 4-16. (In Rus).
14. Petrenko S. Self-healing cloud computing // Voprosy Kiberbezopasnosti. 2021. № 1(41). P. 80-89. DOI: 10.21681/2311-3456-2021-1-80-89.
15. Kharzhevskaya A. V., Lomako A. G., Petrenko S. A. Representing programs with similarity invariants for monitoring tampering with calculations. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017. № 2(20). Pp. 9-20. (In Rus). DOI: 10.21581/2311-3456-2017-2-9-20.

16. Vorobyov E. G., Petrenko S. A., Olaode J. A., Alshanskaya T. V. Metodika samovosstanovlenija vychislenij v uslovijah vozmushhenij [Self-restoration computational method in the condition of disturbance]. Materialy Mezhdunarodnoj konferencii po mjagkim vychislenijam i izmerenijam [Proceedings of the XXV International Conference on Soft Computing and Measurements. Saint-Petersburg, 2018]. Sankt-Peterburg, 2018. Pp. 298-299. (In Rus).
17. Mirzabaev A. N., Samonov A. V. Control method of the correct execution of programs by monitoring and analyzing the real-time parameters of the computing process. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2022. № 2(48). Pp. 63-71. (In Rus). DOI 10.21681/2311-3456-2022-2-63-71.
18. Balyabin A. A., Petrenko S. A., Yakimovskaya R. N. Algoritm pasportizacii vychislenij SAP HANA na osnove razmernostej [SAP HANA passportization algorithm based on dimensions]. Materialy IX mezhdunarodnoj nauchno-prakticheskoj konferencii «Povyshenie konkurentosposobnosti social'no-jekonomicheskih sistem v uslovijah transgranichnogo sotrudnichestva regionov» [Proceedings of the IX International Conference «Increasing the competitiveness of socio-economic systems in the context of cross-border cooperation between regions», Yalta, on April 05-08, 2022]. Simferopol, 2022. Pp. 68-71. (In Rus).
19. Balyabin A. A., Petrenko S. A., Antonov V. V. Algoritm obnaruzhenija anomalij funkcionirovanija SAP HANA na osnove razmernostej [SAP HANA anomaly detection algorithm based on dimentions]. Materialy IX mezhdunarodnoj nauchno-prakticheskoj konferencii «Povyshenie konkurentosposobnosti social'no-jekonomicheskih sistem v uslovijah transgranichnogo sotrudnichestva regionov» [Proceedings of the IX International Conference «Increasing the competitiveness of socio-economic systems in the context of cross-border cooperation between regions», Yalta, on April 05-08, 2022]. Simferopol, 2022. Pp. 61-64. (In Rus).
20. Balyabin A. A., Petrenko S. A., Golumbovskaya A. N. Algoritm vyjavlenija anomalij funkcionirovanija sistemnyh prilozhenij v uslovijah otsutstvija ishodnyh kodov [Algorithm of anomaly detection for system applications in the absence of source codes]. Materialy IX mezhdunarodnoj nauchno-prakticheskoj konferencii «Povyshenie konkurentosposobnosti social'no-jekonomicheskih sistem v uslovijah transgranichnogo sotrudnichestva regionov» [Proceedings of the IX International Conference «Increasing the competitiveness of socio-economic systems in the context of cross-border cooperation between regions», Yalta, on April 05-08, 2022]. Simferopol, 2022. Pp. 65-68. (In Rus).