Платформа (SDK) для самовосстановления специальной микроядерной операционной системы (KasperskyOS, QNX, Minix, osFree) на основе кибериммунитета

А. А. Балябин[1], С. А. Петренко[2]
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
[1]treven.wt@yandex.ru, [2]s.petrenko@rambler.ru

***Аннотация*. В статье рассмотрена платформа для самовосстановления специальных микроядерных операционных систем на основе кибериммунитета. Данная платформа предназначена для обеспечения требуемой киберустойчивости цифровых платформ путем решения различных задач информационной безопасности: выявления и классификации штатного и аномального функционирования операционных систем; поиска шаблонов вредоносных воздействий; реагирования на компьютерные инциденты; самовосстановления машинных вычислений; адаптивного управления кибербезопасностью; синтеза новых знаний кибербезопасности и пр. Проведена оценка эффективности различных методов обнаружения аномалий.**

Ключевые слова: кибербезопасность; киберустойчивость; искусственная иммунная система; предупреждение кибератак; модели и методы искусственного интеллекта; самовосстановление

I. Введение

В настоящее время в условиях беспрецедентного роста количества угроз безопасности и кибератак злоумышленников становится очевидной недостаточная эффективность существующих классических алгоритмов, методов и средств защиты информации. Так критическая информационная инфраструктура Российской Федерации выстраивается на основе современных цифровых технологий и имеет высокую структурно-функциональную сложность. Многоуровневая организация инфраструктуры снижает ее прозрачность и усложняет интеллектуальное управление. Как следствие, возникает потенциальная опасность наличия скрытых деструктивных программно-аппаратных закладок и уязвимостей на различных уровнях системы.

II. Постановка задачи

Применяемые на сегодняшний день подходы к обеспечению надежности и отказоустойчивости (реконфигурация, n-кратное резервирование, сравнение с эталоном) не способны предотвратить возможные критические последствия для информационной инфраструктуры в случае реализации таких уязвимостей. Кроме этого, постоянно появляются новые уязвимости, способы обхода средств защиты и способы атаки. В соответствии с результатами исследований, приведенными в [1], около 40 % от общего количества кибератак являются новыми, ранее неизвестными кибератаками, которые не могут быть обнаружены.

Очевидно, что появление новых уязвимостей и способов их эксплуатации неизбежно ввиду постоянного роста сложности программного и аппаратного обеспечения информационных систем. С другой стороны, очевидна необходимость обеспечения требуемой их устойчивости и надежности.

С учетом данного противоречия перспективной является идея использования биоинспирированных подходов, в частности, наделения информационных систем свойствами иммунитета по аналогии с иммунитетом живого организма, для эффективного противодействия как известным, так и ранее неизвестным кибератакам злоумышленников, и упреждения их катастрофических последствий. Принципиальное отличие этого подхода от существующих заключается в наличии способности накапливать «иммунную память» к уже встречавшимся и вновь появляющимся кибератакам, планировать «иммунный ответ» и осуществлять самовосстановление систем в реальном времени.

III. Критический анализ методов обнаружения аномалий

В настоящее время выделяют три больших класса методов обнаружения аномалий: сигнатурные, корреляционные и инвариантные [1].

Сигнатурные методы характеризуются наличием строго заданной модели корректного или злоумышленного воздействия. Отклонения от такой модели, как в случае корректного воздействия, так и в случае заведомо вредоносного, либо не анализируются, либо приводят к возникновению ошибок I-го и II-го рода, в зависимости от политики анализа. Таким образом, недостатком, очевидно, является принципиальная невозможность обнаружения новых, ранее неизвестных воздействий злоумышленников. Однако, сигнатурные методы обладают и преимуществами, к которым можно отнести отсутствие ложных срабатываний внутри области, описываемой моделью.

Корреляционные методы используют определенные метрики, которые позволяют определить степень отличия наблюдаемого множества (вектора) признаков от множества (вектора), соответствующего заведомо корректному или злоумышленному воздействию. Иногда

данные методы также используют характеристики более сложной природы, например, поведенческие. К очевидным достоинствам корреляционных методов можно отнести полное покрытие допустимого множества воздействий, что может позволить обнаруживать и ранее неизвестные вредоносные воздействия. Однако, данные методы обладают высоким уровнем ложных срабатываний.

Инвариантные методы накладывают ограничения на пространство признаков таким образом, чтобы включить все множество корректных состояний и одновременно минимизировать долю вредоносных воздействий, удовлетворяющих данным ограничениям. Таким образом инвариантные методы позволяют спроектировать систему обнаружения аномалий, способную обнаруживать новые типы воздействий при минимальном уровне ложных срабатываний.

Сводная таблица достоинств и недостатков рассмотренных классов методов обнаружения аномалий представлена в табл. 1.

ТАБЛИЦА I ПРЕИМУЩЕСТВА И НЕДОСТАТКИ МЕТОДОВ ОБНАРУЖЕНИЯ АНОМАЛИЙ

Методы	Преимущества	Недостатки
Сигнатурные методы	отсутствуют ложные срабатывания внутри области, описываемой моделью	практически не способны обнаруживать аномалии, не заложенные в базу сигнатур
Корреляционные методы	способны обнаруживать аномалии, не заложенные в базу	обладают высоким уровнем ложных срабатываний
Инвариантные методы	способны обнаруживать новые (ранее не встречавшиеся) типы аномалий; отсутствуют ложные срабатывания	не способны обнаруживать атаки, не вызывающие нарушение семантичесской корректности

Таким образом, с целью эффективного обнаружения известных и ранее неизвестных атак злоумышленников с учетом минимизации ошибок I-го и II-го рода перспективными являются методы, основанные на инвариантах.

IV. МЕТОДЫ КИБЕРИММУНИТЕТА ДЛЯ ВЫЯВЛЕНИЯ И КЛАССИФИКАЦИИ АНОМАЛИЙ

В основе методов кибериммунитета, предлагаемых для использования с целью обнаружения вторжений и аномалий, лежит математическая модель иммунного ответа, разработанная академиком Г. И. Марчуком [2]. Такая аналогия с иммунной системой живого организма проводится для придания системам обнаружения аномалий способности обнаруживать ранее неизвестные атаки, адаптироваться и накапливать «иммунную память», а также противодействовать атакам и осуществлять самовосстановление.

В основе известных искусственных иммунных систем, применяемых для обнаружения и противодействия компьютерным атакам, лежит модельное представление о взаимодействии вида «антиген-антитело» из классической иммунологии. Под антигенами в кибериммунных системах понимают деструктивные фрагменты программного кода, некорректные сетевые пакеты и др. Под антителами – микропрограммы восстановления корректности функционирования системы [1]. Наибольший интерес с точки зрения обеспечения адаптивности и самоорганизации, а также обеспечения возможности распознавания неизвестных ранее атак, представляют отрицательный отбор и клональная селекция.

A. Отрицательный отбор

Алгоритм отрицательного отбора, предложенный С. Форрест в работе [3], лег в основу исследований искусственных иммунных систем с точки зрения генерации и селекции иммунных детекторов, предназначенных для распознавания «своих» и «чужих» элементов компьютерных систем. На рис. 1 представлена упрощенная концептуальная модель процесса обучения и распознавания на основе иммунных детекторов, где алгоритм отрицательного отбора главным образом применяется на этапе обучения.

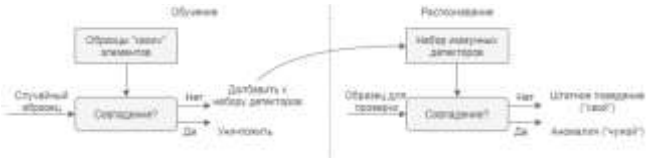

Рис. 1. Упрощенная концептуальная модель обучения и распознавания на основе иммунных детекторов

Пусть имеется некоторое пространство признаков U, множество элементов, классифицируемых как «свои» – S, множество элементов, классифицируемых как «чужие» – N, причем:

$$\begin{cases} U = S \cup N; \\ S \cap N = \varnothing. \end{cases}$$

Требуется:

- определить подмножество S элементов длины l множества U (например, если U представляет множество всех возможных состояний системы, то S – подмножество, состоящее из состояний, определяющих штатное ее функционирование);
- задать множество D детекторов, таких, чтобы каждый из детекторов не распознавал элементы из S;
- осуществлять контроль изменения состояния системы путем проверки состояний S на наборе детекторов D до тех пор, пока не будет найдено соответствие (активация прошедшего отбор детектора на каком-либо состоянии говорит о наличии изменений в системе, относящихся к «чужим»).

Активация бинарного детектора определяется на основе правила: если $x = x_1 x_2 ... x_n$ – двоичная строка длины n, $d = d_1 d_2 ... d_n \in D$ – детектор в виде двоичной последовательности длины n, то

$$x \; matches \; d \equiv \exists i \le n - r + 1 : x_j = d_j \forall j \in \overline{i,...,i+r-1},$$

означающего, что детектор d активируется элементом x (d распознает x), если в бинарном представлении

этих строк есть подстрока из r бит, такая, что каждый бит подстроки детектора совпадает с соответствующим битом подстроки распознаваемого элемента.

B. Клональная селекция

В основе данного подхода лежит теория клональной селекции и приобретаемого иммунитета Ф. Бернет [4] (1959). Когда антитела на поверхности В-клеток связываются с антигенами, В-клетка начинает размножаться. Сначала дочерние В-клетки являются копиями родительских, далее они претерпевают некоторые изменения, называемые соматическими гипермутациями. Производимые ими антитела оказываются специфичными к конкретному антигену и направлены на его уничтожение. Таким образом осуществляется адаптивный иммунный ответ и формируется иммунная память.

Рассмотренный ранее алгоритм отрицательного отбора позволяет сгенерировать набор антител для борьбы с уже известными антигенами. Однако, биологическая иммунная система обладает способностью противостоять и ранее неизвестным угрозам, обучаясь на новых антигенах и формируя иммунную память. В рамках искусственной иммунной системы для этого применяется алгоритм клональной селекции.

Пусть Ag – множество антигенов, Ab – множество антител, f – вектор длины N значений аффинности антигена и всех существующих антител. Тогда последовательность шагов алгоритма в общем случае выглядит следующим образом:

- для вновь обнаруженного антигена $Ag_j \left(Ag_j \in Ag \right)$ вычисляется его аффинность для всех существующих антител Ab;
- в вектор значений аффинности $f = \left\{ f_j \right\}$ длины N заносятся результаты вычислений из предыдущего пункта;
- проводится выбор $n < N$ максимальных значений аффинности, формируется новое множество $Ab^j_{\{n\}}$ из соответствующих антител из Ab;
- n выбранных антител клонируются пропорционально значению их аффинности к антигену Ag_j (чем больше степень аффинности, тем больше клонов). Из клонированных элементов формируется множество C^j;
- элементы множества C^j проходят процедуру мутации, причем число мутирующих генов в антигене пропорционально его аффинности с антигеном Ag_j. Формируется множество C^{j*} клонов антител, прошедших мутацию;
- вычисляется аффинность f^{j*} прошедших мутацию клонов из множества C^{j*} по отношению к антигену Ag_j;
- среди элементов множества C^{j*} выбирается антитело Ab^*_j, имеющее максимальную аффинность к антигену Ag_j. Если аффинность выбранного антитела по отношению к антигену Ag_j больше любого элемента вектора f, то такое антитело добавляется в иммунную память.

Обобщенный алгоритм клональной селекции приведен на рис. 2.

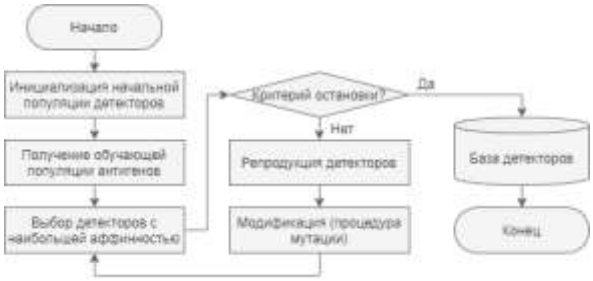

Рис. 2. Обобщенный алгоритм клональной селекции с мутацией

V. Архитектура платформы для самовосстановления микроядерной операционной системы на основе кибериммунитета

Выделяют три основных типа операционных систем:

- монолитные;
- микроядерные;
- гибридные.

В данной работе предлагается платформа восстановления операционной системы на основе свойств кибериммунитета применительно к микроядерным операционным системам, архитектура которой приведена на рис. 3.

Подсистема мониторинга предназначена для обнаружения вредоносных воздействий, на основе использования так называемых иммунных детекторов. Иммунные детекторы генерируются и обучаются при помощи приведенных ранее алгоритмов отрицательного отбора и клональной селекции. При этом, детекторы являются чувствительными к изменению семантической корректности выполняемых в операционной системе программ. Это достигается за счет задания семантических инвариантов и правил их контроля [1, 5–6].

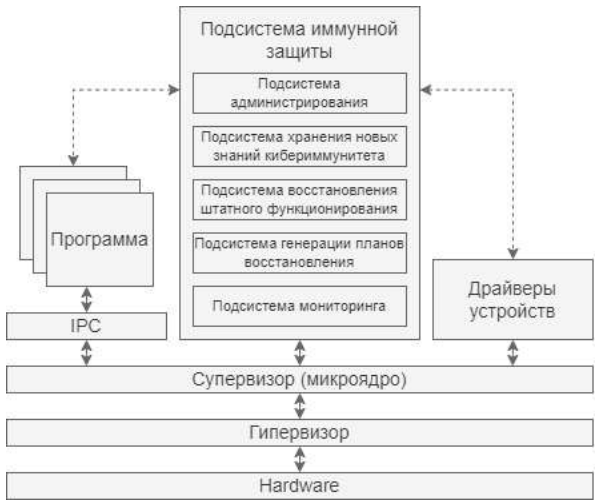

Рис. 3. Архитектура платформы самовосстановления микроядерной операционной системы

Подсистема генерации планов восстановления отвечает за синтез микропрограмм восстановления, используемых в дальнейшем подсистемой восстановления штатного функционирования операционной системы.

В процессе функционирования кибериммунной системы защиты, противодействия выявляемым кибератакам злоумышленников, в системе появляется информация о типах и характеристиках воздействия. Для ее накопления с целью более оперативного распознавания и реагирования на угрозы в будущем, в систему иммунной защиты входит подсистема хранения новых знаний кибериммунитета. Она является реализацией механизма накопления так называемой «иммунной памяти».

Представленные компоненты также могут быть использованы при встраивании в транслятор (компилятор) для придания программам свойств кибериммунитета и способности восстанавливаться при обнаружении ими вредоносных программных воздействий.

VI. Оценка результативности обнаружения аномалий и восстановления ОС

На рис. 4 приведены результаты измерения количества ложных пропусков и ложных срабатываний для трех рассмотренных ранее групп методов.

На основании полученных данных об ошибках I-го и II-го рода следует отметить следующее:

- инвариантные методы имеют преимущество по сравнению с сигнатурными в виде меньшей доли ложных пропусков аномалий, не занесенных в базу данных сигнатур;
- инвариантные методы обнаружения аномалий имеют преимущество по сравнению с корреляционными методами в виде меньшей доли ложных срабатываний;
- при определенных настройках корреляционные методы позволяют обнаруживать большую долю атак, что, однако, приводит к повышению количества ложных срабатываний.

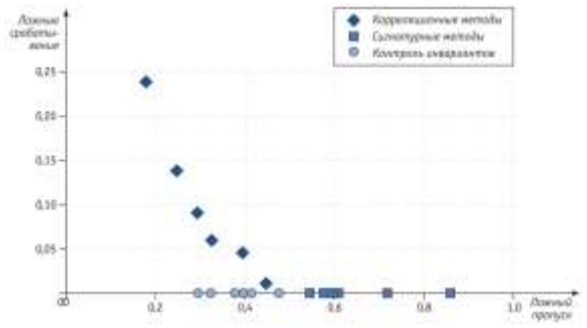

Рис. 4. Характеристики обнаружения аномалий (атак) на плоскости «ложный пропуск/ложное срабатывание» для трех групп методов

Таким образом, несмотря на очевидные преимущества инвариантных методов, вероятно, наиболее оправданным с точки зрения полноты покрытия пространства признаков и минимизации ошибок I-го и II-го рода для различных типов воздействий было бы применение на базе предложенной платформы самовосстановления гибридных методов обнаружения, заключающихся в совместном использовании всех трех методов [5].

VII. Заключение

Предложенная в работе платформа самовосстановления микроядерных операционных систем позволит выявлять аномалии поведения систем, возникшие в результате деструктивных воздействий (в том числе и ранее неизвестных, за счет реализации механизмов иммунной защиты), противодействовать им, осуществлять самовосстановление параметров поведения, влияющих на киберустойчивость системы, а также накапливать знания о воздействиях для повышения эффективности реализации «иммунного ответа» на вторжения в будущем.

Список литературы

[1] Петренко С.А. Кибериммунология: научная монография. СПб: «Издательский Дом «Афина». 2021. 240 с.

[2] Марчук Г.И. Математические модели в иммунологии: вычислительные методы и эксперименты. М.: Наука. 1991. 299 с.

[3] S. Forrest A.S. Perelson L. Allen, and R. Cherukuri. Self-nonself discrimination in a computer. In Proceedings of the 1994 IEEE Symposium on Security and Privacy, page 202. IEEE Computer Society, 1994.

[4] Burnet F.M. The Clonal Selection Theory of Acquired Immunity. Great Britain, Cambridge: The University Press, 1959. 232 p.

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

[6] Зотова А.В. Способ паспортизации расчетных алгоритмов программ / А.В. Зотова, Р.И. Компаниец, В.В. Ковалев // Защита информации. Инсайд. 2016. № 5(71). С. 26-33.