УДК 621.34

С.Ю. Гавриленко, А.А. Горносталь

Национальный технический университет «ХПИ», Харьков

РАЗРАБОТКА АДАПТИВНЫХ ШАБЛОНОВ ФИКСАЦИИ АНОМАЛЬНОГО ПОВЕДЕНИЯ КОМПЬЮТЕРНОЙ СИСТЕМЫ

В работе разработаны адаптивные шаблоны фиксации аномального поведения компьютерной системы. Рассмотрена возможность использования для этих целей контрольных карт Шухарта. На основе контрольных карт Шухарта разработана программная модель, формирующая базу шаблонов нормального состояния компьютерной системы. Проведены исследования, с использованием вредоносного программного обеспечения типа «thread creater», которые показали работоспособность системы выявления аномалий на основе разработанных адаптивных шаблонов фиксации.

Ключевые слова: *компьютерные системы, адаптивные шаблоны фиксации аномального поведения, карты Шухарта.*

Постановка задачи

В условиях постоянной опасности киберпреступлений, динамического роста разновидностей вредоносного программного обеспечения все актуальнее встает вопрос совершенствования существующих средств предупреждения и обнаружения вторжений в компьютерные системы (КС), в основу которых чаще всего входят сигнатурные и эвристические анализаторы. При этом в связи с ограниченными возможностями сигнатурных анализаторов аномального поведения все больший объем функций возлагается на эвристические анализаторы.

Эвристические анализаторы, как правило, включают в себя интеллектуальные подсистемы, базирующиеся на теории искусственного интеллекта, например, на основе методов нечеткой логики, кластерного анализа, согласованных эвристик или теории нейронных сетей [4 – 5]. В то же время все они основаны на предположении, что для КС существует свой шаблон нормального поведения и любые значительные отклонения от него могут быть обусловлены воздействием злоумышленников. Именно поэтому очень важной задачей является выбор или формирование такого шаблона, который бы воспроизводил функциональный портрет КС и фиксировал аномальное ее поведение с заданной точностью.

Анализ литературы показал, что для построения шаблона КС в настоящее время могут применяться контрольные карты Шухарта, EWMA и CUSUM [1, 6 – 8], использующие в качестве входных данных набор показателей, характеризующий нормальную работу системы. Кроме этого для уточнения полученных результатов дополнительно могут использоваться методы статистической обработки данных (например, BDS-тестирование) [7].

Однако, как показали исследования, приведенные средства формирования шаблонов не лишены ряда недостатков. Так, например, контрольные карты EWMA нечувствительны к коротким проявлениям аномалий. В то же время карты CUSUM обнаруживают небольшие, но постоянные изменения с большей вероятностью, но обладают низкой точностью (высокой вероятностью ложных срабатываний) в случае динамических изменения показателей КС.

Устранить это противоречие можно разработкой адаптивных шаблонов фиксации аномального поведения КС.

Основная часть

Проведенный анализ, показал, что одним из перспективных направлений разработки адаптивных шаблонов состояния КС является использование контрольных карт Шухарта (ККШ) [6 – 8].

Как показали исследования, контрольные карты Шухарта эффективно обнаруживают случайные и большие отклонения от заранее заданного критерия и представляет собой визуальный инструмент – график изменения параметров процесса во времени [6 – 8].

Проведенные исследования процесса функционирования КС показали частые флуктуационные изменения характеристических показателей (загрузка центрального процессора (ЦП) и оперативной памяти (ОП) и др.) вследствие воздействия различных факторов. Таких факторов обычно много, и поэтому они частично компенсируют друг друга. Вследствие этого в стабильном состоянии выходы процесса лежат в определённом коридоре – зоне системной вариабельности процесса. Вероятность выхода параметра за пределы этого коридора не равна нулю, но, как правило, мала.

Выделяют основные признаки, сигнализирующие о выходе процесса из стабильного состояния:

– выход точек за верхнюю или нижнюю границы контрольной карты;

– 7 или более точек подряд лежат по одну сторону от средней линии;

– более 6 точек монотонно возрастают или убывают.

Аномальное поведение работы КС связано з выполнением злоумышленных действий, приводящих к нарушению работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей, приведение в негодность аппаратных комплексов компьютера.

Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы, такие как оперативную память, перегружают работу центрального процессора и сетевой карты.

В ходе исследования было принято решение в качестве изучаемых показателей выбрать загрузку ЦП и объём используемой ОП. При этом данные показатели решено брать в относительных единицах (в %), так как это позволит не привязываться к конкретным аппаратным особенностям той или иной системы, а сосредоточиваться на нахождении общих закономерностей.

Выбор показателей обусловил использование количественного вида контрольных карт. В качестве выборочного параметра карты использовалось среднее значение [6].

Как известно, ККШ строятся как графики зависимостей некоторых величин. При этом аргументом функции чаще всего выступает время, а значением – отношение изучаемых показателей.

В нашей модели ось абсцисс является временной шкалой, а по оси ординат отложено отношение загрузки центрального процессора к проценту используемой памяти X.

Полученные ККШ содержат 3 основные линии:

– среднее значение (среднее арифметическое полученных $\overline{X}$);

– верхняя контрольная граница (рассчитывается по формуле $\overline{X}+\overline{R}\cdot A_2$, где $\overline{R}$ – средний размах, а A_2 – табличный коэффициент, выбираемый в зависимости от количества экспериментов);

– нижняя контрольная граница (рассчитывается по формуле $\overline{X}-\overline{R}\cdot A_2$ с аналогичными величинами).

Для проведения эксперимента была разработана модель для обнаружения аномального поведения компьютерной системы на основе ККШ (рис. 1), где X – загрузка центрального процессора и Y – объём используемой оперативной памяти, X/Y – их отношение.

Загрузка центрального процессора и оперативной памяти сканируются посекундно и сохраняются в файле.

Количественное значение временного ряда может варьироваться.

На первом этапе формируется база шаблонов различных режимом работы КС, при этом результатом работы блока формирования шаблона являются среднее значение, верхняя и нижняя контрольная граница, а также график, характеризующий состояние системы.

На последующем этапе происходит сравнение контрольных карт Шухарта, полученных в реальном режиме времени для определенной модели с ее шаблоном, хранящимся в базе шаблонов.

На основании результата работы блока сравнения принимается решение о состоянии КС.

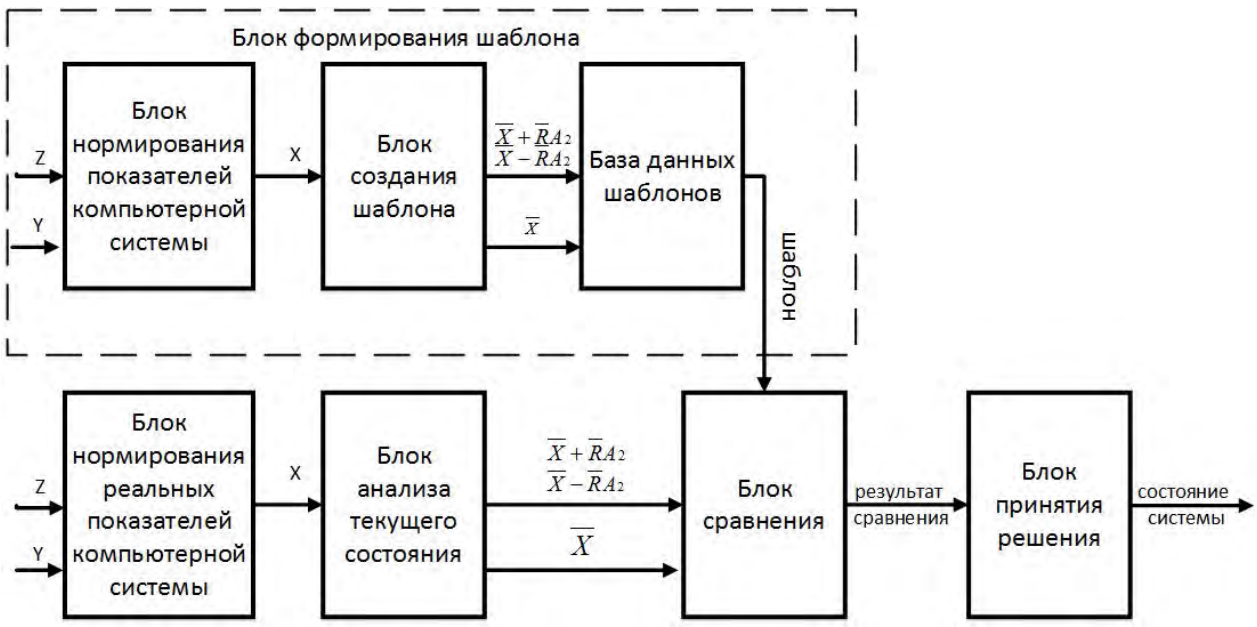


Рис. 1. Структурная схема системы формирования шаблонов и выявления аномального поведения КС

Для проведения эксперимента была разработана программная модель для обнаружения аномального поведения компьютерной системы на основе контрольных карт Шухарта.

На рис. 2, 3 приведены шаблоны, полученные для двух режимов: «Офисный работник» и «Студент-программист». Каждый режим характеризуется определённым набором запущенных программ.

Как видно из графиков, основные признаки, сигнализирующие о выходе процесса из нормального состояния, не нарушены.

На рис. 4, а показано состояние системы для режима «Офисный работник» в условиях запуска разработанного вредоносного программного обеспечения типа «thread creater» (вредоносное программное обеспечение запущено на 15 сек.).

Как видно из рис. 4, а среднее значение и границы ККШ для данной системы изменились, значение выбранных показателей, характеризующих процесс функционирований КС, не вышло за границы коридора, но вместе с тем по одну сторону от средней линии подряд лежат более 7 точек.

На рис. 4, б показано состояние КС для режима ««Студент-программист» в условиях, аналогичных предыдущему эксперименту. Среднее значение и границы контрольной карты Шухарта для КС также изменились, значение процесса не вышло за границы коридора и по одну сторону от средней линии подряд лежат более 7 точек.

На рис. 5 отображено наложение графического отображения функционального портрета КС на ее шаблон.

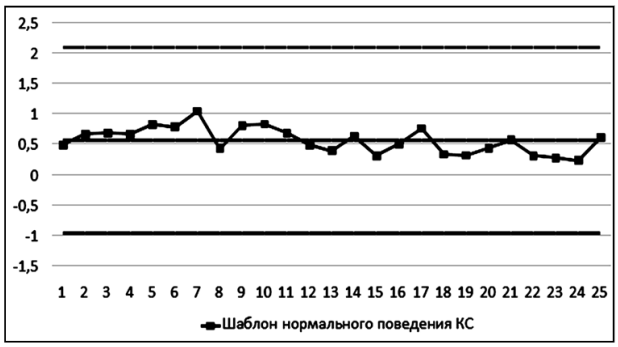
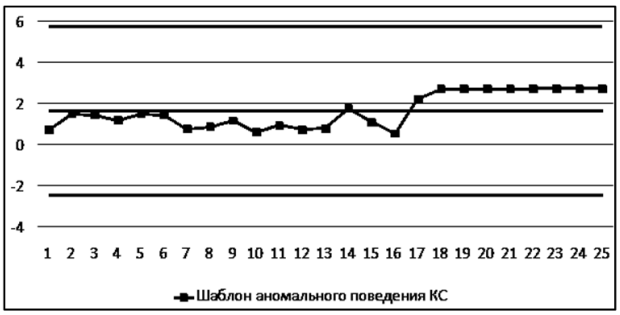
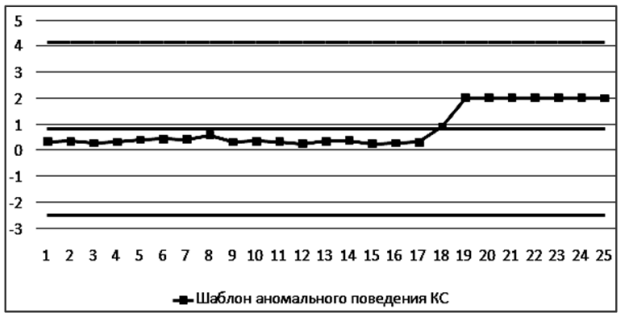


Рис. 2. Режим «офисный работник»

Рис. 3. Режим «студент-программист»

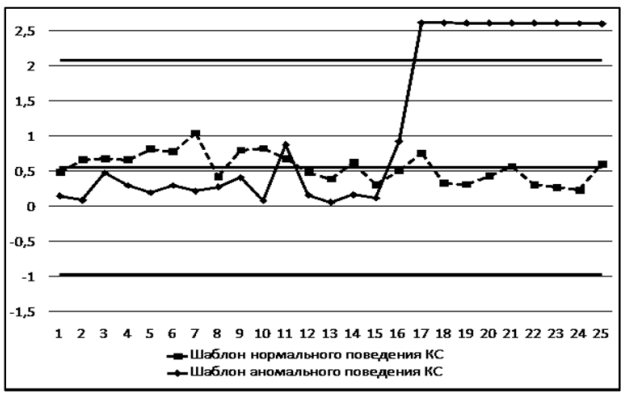


а – режим «Офисный работник»

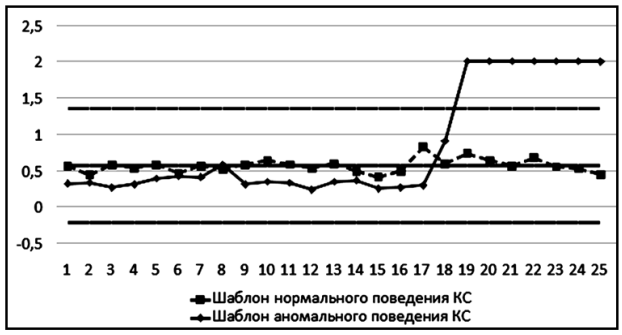


б – режим «Студент-программист»

Рис. 4. Контрольная карта Шухарта для зараженной системы



а – режим «Офисный работник»



б – режим «Студент-программист»

Рис. 5. Совмещение графического отображения функционального портрета зараженной КС с шаблоном

Как видно из графиков рис. 5, кроме наличия подряд более 7 точек, фиксируется выход точек зараженной системы за верхнюю границу контрольной карты шаблона.

Выводы

Таким образом, в статье разработаны адаптивные шаблоны фиксации аномального поведения компьютерной системы. Подтвержден факт возможности использования для этих целей контрольных карт Шухарта.

Для разработки и экспериментальных исследований разработана программная модель, позволяющая получить базу шаблонов состояния компьютерной системы и осуществить фиксацию анормальности поведения КС.

Исследования, проведенные с использованием вредоносного программного обеспечения типа «thread creater» показали работоспособность системы выявления аномалий на основе разработанных адаптивных шаблонов фиксации.

Полученные результаты исследований позволяют сделать вывод о возможности использования разработанных адаптивных шаблонов фиксации аномального поведения состояния компьютерной системы в эвристических анализаторах систем обнаружения вторжений

Список литературы

1. Обнаружение вторжений в компьютерные сети. – М.: Грячая линия-Телеком, 2013. – 220 с.

2. Общие сведения о картах кумулятивных сумм. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.stattools.net/CUSUM_Exp.php.

3. Оссовский С. Нейронные сети для обработки информации / Станислав Осовский; пер. с польского И.Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с.

4. Джон Сноу. Вирус на блюдечке [Электронный ресурс]. – Режим доступа к ресурсу: https://xakep.ru/2002/02/18/14534/.

5. Матвеев И.В. Классификация компьютерных вирусов. Примеры вирусов [Электронный ресурс]. – Режим доступа к ресурсу: http://dom8a.ru/seminar-ib/05.06.2014/matveev/paper.pdf.

6. Государственный стандарт Российской Федерации. Статистические методы. Контрольные карты Шухарта [Электронный ресурс]. – Режим доступа к ресурсу: http://pqm-online.com/assets/files/lib/ std/gost_r_50779.42-1999.pdf.

7. Семенов С.Г. Защита данных в компьютеризированных управляющих системах (монография) / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – Изд. «LAP LAMBERT ACADEMIC PUBLISHING» Германия, 2014. – 236 с.

8. Уилер Дональд, Чамберс Дэвид. Статистическое управление процессами: Оптимизация бизнеса с использованием контрольных карт Шухарта = Understanding Statistical Process Control. – М.: Альпина Паблишер, 2009. – 310 с. – ISBN 978-5-9614-0832-4.

9. Лапидус В.А. Система Шухарта / В.А. Лапидус. – Н.Новгород: ООО СМЦ "Приоритет", 2004.– 65 с. – ISBN 5-98366-010-1.

Поступила в редколлегию 29.02.2016

Рецензент: д-р техн. наук, ст. научн. сотр. С.Г. Семенов, Национальный технический университет «ХПИ», Харьков.

РОЗРОБКА АДАПТИВНИХ ШАБЛОНІВ ФІКСАЦІЇ АНОМАЛЬНОЇ ПОВЕДІНКИ КОМП'ЮТЕРНОЇ СИСТЕМИ

С.Ю. Гавриленко, О.А. Горносталь

У роботі розроблені адаптивні шаблони фіксації аномальної поведінки комп'ютерної системи. Розглянуто можливість використання для цих цілей контрольних карт Шухарта. На основі контрольних карт Шухарта розроблено програмну модель, що формує базу шаблонів нормального стану комп'ютерної системи. Проведено дослідження, з використанням шкідливого програмного забезпечення типу «thread creater», які показали працездатність системи виявлення аномалій на основі розроблених адаптивних шаблонів фіксації.

***Ключові слова**: комп'ютерні системи, імітаційна модель, карти Шухарта, зовнішні впливи на комп'ютерну систему.*

DEVELOPMENT THE ADAPTIVE TEMPLATES FOR FIXING OF THE ANOMALOUS BEHAVIOR OF THE COMPUTER SYSTEM

S.Yu. Gavrilenko, O.A. Hornostal

The paper considers the possibility of using Shewhart control charts to detect anomalous behavior of the computer system. A software model that was developed creates the templates` base of the computer system`s states based on Shewhart control charts (SCC). It fixes abnormal behavior of the computer system by the pattern matching. This article also contains analysis of the simulation results.

***Keywords:** computer systems, simulation model, maps Shewhart, external influences on the computer system.*