2. Лукашкин, К.А. Проблемы безопасности программного обеспечения военной техники [Электронный ресурс] / К.А. Лукашкин // Военное дело. – 2001. – Режим доступа: http://www.soldiering.ru/psychology/safe_soft_militaryequip.php. – Дата доступа: 17.09.2015.
3. Ian A. Finlay. Backdoor in Alcatel OmniSwitch AOS [Электронный ресурс] / Finlay // Carnegie Mellon University. – 2015. – Режим доступа: http://www.cert.org/historical/advisories/CA-2002-32.cfm. – Дата доступа: 20.09.2015.
4. Группа компаний InfoWatch [Электронный ресурс] / InfoWatch. – 2015. – Режим доступа: https://www.infowatch.ru/sites/default/files/files/products/appercut/Appercut_Company_Brochure_Rus.pdf. – Дата доступа: 16.09.2015.

УДК 004.42

ФУНКЦИОНАЛЬНАЯ СТРУКТУРА СИСТЕМЫ БОРЬБЫ С АНОМАЛЬНОЙ АКТИВНОСТЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А.Е. РАМАШКА
(Представлено: канд. техн. наук, доц. К.Я. РАХАНОВ)

Рассмотрена возможная функциональная структура системы для борьбы с аномальной активностью программного обеспечения с применением облачных технологий.

В последнее время, в связи с ростом скорости внедрения информационных технологий в экономику и промышленность, наиболее остро встала проблема защиты конфиденциальных и секретных данных, представляющих определенную ценность, будь то определенные технологии производства или же данные о клиентах.

С точки зрения информационных технологий особую опасность представляют сами средства вычислительной техники в первую очередь компьютеризированные рабочие места сотрудников предприятия [1]. Одним из способов получения несанкционированного доступа к информации является внедрение в программное обеспечение не декларированных возможностей, которые порождают аномальную активность программного обеспечения.

Автоматизированная система должна представлять собой программный комплекс для выявления аномальной активности программного обеспечения, а также устранения возможности изменения информации и несанкционированного доступа к ней.

Система обнаружения аномальной активности должна удовлетворять следующим требованиям:

1) анализировать поведение исследуемого процесса (приложения);
2) возможность сигнатурного анализа исполняемого файла исследуемого процесса;
3) возможность анализа сетевых соединений, открываемых процессом;
4) возможность анализа сетевого трафика, генерируемого приложением;
5) реализация принятия решений оператором и в автоматическом режиме;
6) отвечать требованиям отказоустойчивости (сбой работы элемента системы, атаки на злоумышленников на ресурсы системы);
7) сохранение высокой производительности при пиковых нагрузках;
8) балансировка нагрузки между несколькими модулями обнаружения угроз;
9) низкая нагрузка на аппаратные мощности и ресурсы вычислительной машины;
10) поддержка облачных вычислений.

Исходя из вышеперечисленных требований система состоит из компонентов:

1) подсистема получения информации о сетевой активности приложений;
2) подсистема перехвата сетевых пакетов;
3) подсистема контроля целостности системы;
4) подсистема обнаружения угроз;
5) подсистема автоматического реагирования;
6) подсистема распределения нагрузки;
7) подсистема удаленного управления;
8) подсистема администрирования;
9) подсистема авторизации.

Подсистема получения информации о сетевой активности предназначена для постоянного мониторинга всех процессов на компьютере пользователя, а также получения данных о сетевых подключениях, инициированных этими процессами.

Подсистема перехвата сетевых пакетов предназначена для сбора данных о всех сетевых пакетах, генерируемых или получаемых процессами на компьютере пользователя.

Подсистема контроля целостности системы предназначена для мониторинга состояния системы. В случае аварийного или несанкционированного завершения работы одного из компонентов системы, данная подсистема оперативно восстанавливает работоспособность измененного файла.

Подсистема обнаружения угроз – ядро всей системы, которое отвечает за анализ событий, собранных подсистемой сетевой активности приложений и подсистемой перехвата сетевых пакетов.

Подсистема автоматического реагирования отвечает за действия, предпринимаемые по результатам анализа подсистемы обнаружения угроз.

Подсистема распределения нагрузки отвечает за распределение задач анализа и принятия решений равномерно между всеми компьютерами в сети в ситуации, когда серверу не хватает аппаратных ресурсов либо выхода его из строя. Данная подсистема автоматически, при нагрузке, многократно превышающей ту, которую может выдержать основной анализатор, распределяет ее по простаивающим клиентским машинам. Балансировка происходит следующим образом: если загрузка центрального процессора сервера больше 80%, подается команда передачи управления всем управляющим службам на клиентских машинах. Управляющая служба вычисляет процент использования центрального процессора и количество свободной оперативной памяти и записывает данное значение в базу данных. Эмпирическим путем была получена формула вычисления количества пользователей, которое в данный момент возможно анализировать:

$$N = RT \cdot \frac{PU_e}{PU_c} \cdot \frac{RA_e}{RA_c}, \quad (1)$$

где PU_e и RA_e – экспериментально полученные значения использования процессора в процентах и количество свободной оперативной памяти, а PU_c и RA_c – текущие значения тех же параметров, RT – количество потоков выполнения центрального процессора.

Подсистема удаленного управления отвечает за автоматическое выполнение команд по блокировке приложений или сетевого трафика со стороны подсистемы автоматического реагирования.

Подсистема администрирования предназначена для возможности функционирования системы в полуавтоматическом режиме, путем выполнения команд администратором систем или офицером безопасности по блокировке приложений или сетевого трафика в зависимости от возникшего события.

Подсистемы обнаружения угроз и принятия решения, выполняясь на удаленном хосте, реализуют концепцию облачных вычислений, пример которых представлен в работе [2], тем самым значительно снижая нагрузку и потребление аппаратных ресурсов, возникающие при анализе.

Таким образом, функциональную структуру системы можно представить в виде схемы, представленной на рисунке.

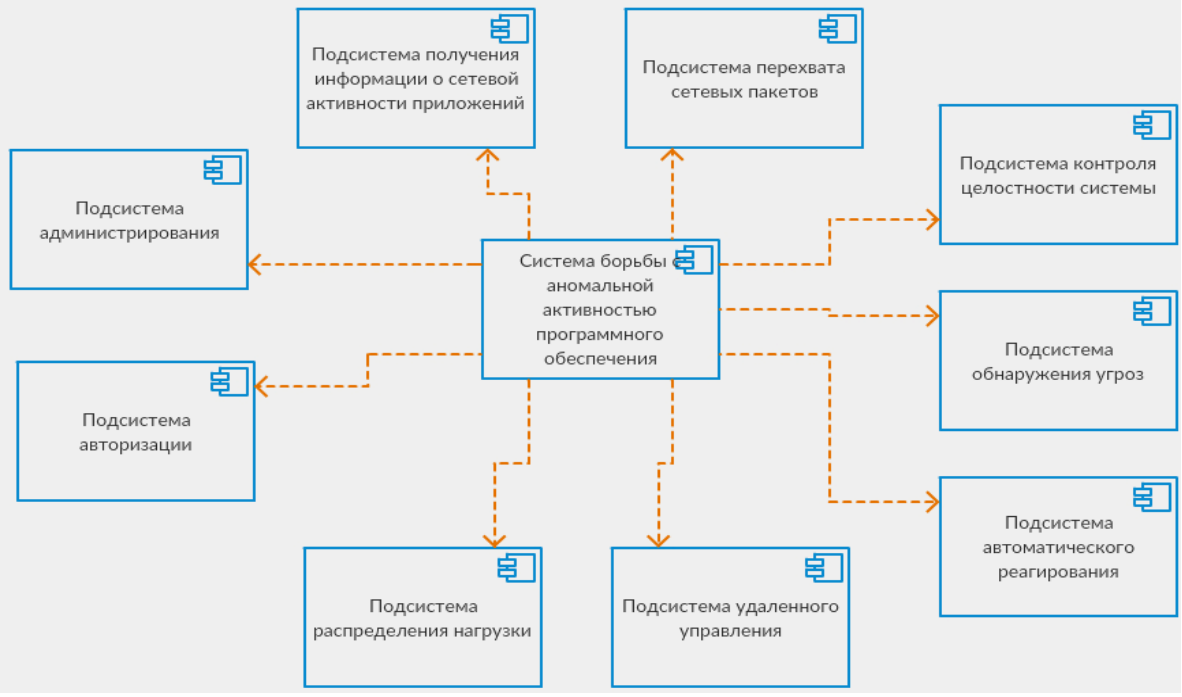

Рис. Функциональная структура автоматизированной системы

Представленная структура описывает базовый функциональный набор и может расширяться в зависимости от специализации.

Выводы. Предложена функциональная структура системы борьбы с аномальной активностью программного обеспечения, которая отличается повышенной надежностью и производительностью за счет применения распределенных вычислений и облачных технологий. Главной отличительной особенностью данной структуры является модульность, благодаря которой, при минимальных затратах, возможно интегрирование дополнительных модулей анализа и реагирования.

ЛИТЕРАТУРА

1. Министерство внутренних дел Республики Беларусь [Электронный ресурс] / Первое российское исследование скрытых угроз, 2011. Режим доступа: http://mvd.gov.by/main.aspx?guid=55533– Дата доступа: 16.09.2015.
2. Орлов С. Облачные сервисы: безопасность и надежность / Журнал сетевых решений №12, 2012 – 10с.

УДК 681.586.773:624.072.233.5

ПРИМЕНЕНИЕ НЕРАЗРУШАЮЩЕЙ ДЕФЕКТОСКОПИИ ДЛЯ КОНТРОЛЯ КАЧЕСТВА ЖЕЛЕЗНОДОРОЖНЫХ РЕЛЬСОВ

П.В. СТЕПАНОВ
(Представлено: канд. техн. наук, доц. Д.А. ДОВГЯЛО)

Рассмотрены наиболее распространенные дефекты, проявляющиеся в процессе производства и эксплуатации железнодорожных рельсов, установлены причины их возникновения. Дана классификация методов неразрушающего контроля, применяемых для бесконтактного или контактного диагностирования скрытых дефектов. Приведено описание оборудования, используемого при ультразвуковой дефектоскопии.

Введение. Неразрушающий контроль (НК) – это контроль, который не разрушает (именно такое определение дано в ГОСТ 16504-81[1]). Под словом «контроль» подразумевается «измерение значений рабочих параметров и свойств объекта и их проверка на соответствие допустимым величинам». «Неразрушающий» означает «не требующий демонтажа или остановки работы объекта», «не подразумевающий непосредственного вмешательства в исследуемую среду». Методы, с помощью которых реализуется НК, называются методами неразрушающего контроля.

Обзор существующих методов НК. На сегодняшний день существует большое разнообразие методов неразрушающего контроля. К ним относятся:

- магнитные методы НК;
- электрические методы НК;
- вихретоковые методы НК;
- радиоволновые методы НК;
- тепловые методы НК;
- оптические методы НК;
- радиационные методы НК;
- акустические методы НК;
- методы НК проникающими веществами.

Данные методы получили развитие в различных отраслях промышленности, использующих НК для диагностики различного рода конструкций, узлов и механизмов. Разновидностью акустических методов НК являются методы, реализованные на основе использования ультразвуковых волн. Ультразвук нашел широкое применение как в научных исследованиях, так и в промышленной технологии после практической реализации надежных способов его возбуждения. В последнее время наряду с традиционной дефектоскопией возрос интерес к ультразвуку как средству контроля физических и механических свойств материалов. При этом если упругие свойства твердых тел аналитически связаны с параметрами упругих волн и могут надежно определяться на основании акустических измерений, то прочностные