УДК 004.457

***К.А. Коновалов***
(Российский Государственный Технологический Университет им. К.Э. Циолковского;
e-mail: kkonov@mail.ru)

# О РЕАЛИЗАЦИИ ПРОГРАММНОГО КОМПЛЕКСА МОНИТОРИНГА И АНАЛИЗА БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ

*Приведён анализ статистических данных по зафиксированным утечкам информации и вирусным атакам на компьютеры различных предприятий. Проведён выбор оптимального алгоритма анализа событий информационной безопасности.*

*Ключевые слова: защита информации, утечки информации, анализ событий.*

***K.A. Konovalov***

# ABOUT THE IMPLEMENTATION OF THE SOFTWARE FOR MONITORING AND ANALYSIS OF COMPUTER NETWORK SECURITY

*Analyzed of statistic data for recorded information leaks and virus attacks on computers of other companies. Selection of the optimal algorithm for the analysis of information security events.*

*Key words: information security, data leakage, analysis of events.*

Статья поступила в редакцию Интернет-журнала 2 июля 2013 г.

Необходимость комплексного подхода к вопросам защиты информации в компьютерных сетях становится все актуальней. Убедиться в этом можно благодаря статистическим отчетам, которые создаются некоторыми организациями, занимающимися разработкой различных средств защиты информации, таких как антивирусы или межсетевые экраны, и организациями, занимающимися исключительно аналитическими исследованиями в отрасли ***ИТ (информационные технологии)***.

Результаты статистических отчетов [1-5] организации InfoWatch, предоставляющей аналитическую информацию по ситуации в отрасли ИТ, по утечкам информации за период с 2006 г. по 2012 г. говорят о том, что количество инцидентов, приведших к утечкам конфиденциальной информации, постоянно возрастает (табл. 1).

Кроме вышеуказанной статистики можно также обратить внимание на отчет компании Symantec [6], в котором приведены данные по созданным для своего антивирусного решения за календарный год сигнатурам для обнаружения таких вредоносных программ, как вирусы и троянские программы в период с 2002 г. по 2009 г. К сожалению в следующем отчете (за 2010 г.) компания убрала статистику по сигнатурам и данные за 2010 г. стало возможно получить только просмотрев, сколько всего существовало сигнатур [7] на момент конца 2009 г. и конца 2010 г. (рис. 1).

Таблица 1

**Утечки конфиденциальной информации по результатам статистических отчётов компании InfoWatch**

| Год / Вид утечек | | Умышленные | Случайные | Не установлено | Всего |
|---|---|---|---|---|---|
| 2012 | Кол-во (%) | 430 (46) | 352 (38) | 152 (16) | 934 |
| 2011 | Кол-во (%) | 344 (43) | 336 (42) | 121 (15) | 801 |
| 2010 | Кол-во (%) | 334 (42) | 420 (53) | 40 (5) | 794 |
| 2009 | Кол-во (%) | 382 (51,1) | 325 (43,5) | 40 (5,4) | 747 |
| 2008 | Кол-во (%) | 223 (42) | 242 (45,7) | 65 (12,3) | 530 |
| 2007 | Кол-во (%) | 295 (88,6) | 38 (11,4) | - | 333 |
| 2006 | Кол-во (%) | 237 (71,2) | 96 (28,8) | - | 333 |

Кроме того, есть данные по сигнатурам компании Symantec за последние пару лет на отдельном аналитическом ресурсе [8]. Также можно получить некоторые данные по состоянию в отрасли ИТ благодаря ежегодным отчётам компании "Лаборатория Касперского" [9-11] (рис. 2), в которых указано общее число зафиксированных атак на ***ИС (информационную систему)***, производимых вредоносными программами через браузер.

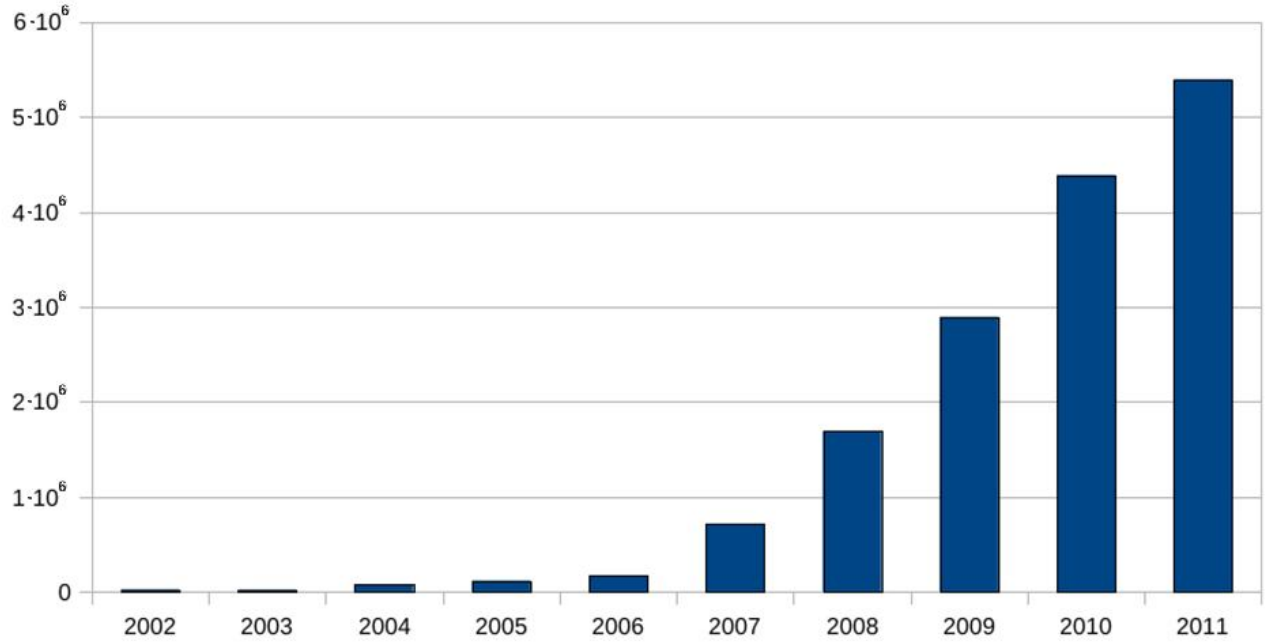


**Рис. 1.** Сигнатуры вирусов, написанные за указанный год компанией Symantec

Проанализировав указанные данные можно без труда увидеть, что ситуация в ближайшие годы в лучшую сторону не изменится: количество компьютеров из года в год увеличивается, всё больше компаний перешло на компьютерную обработку своих данных, вирусов создают всё больше злоумышленников,

а атак на ИС производят с каждым годом всё большее количество.

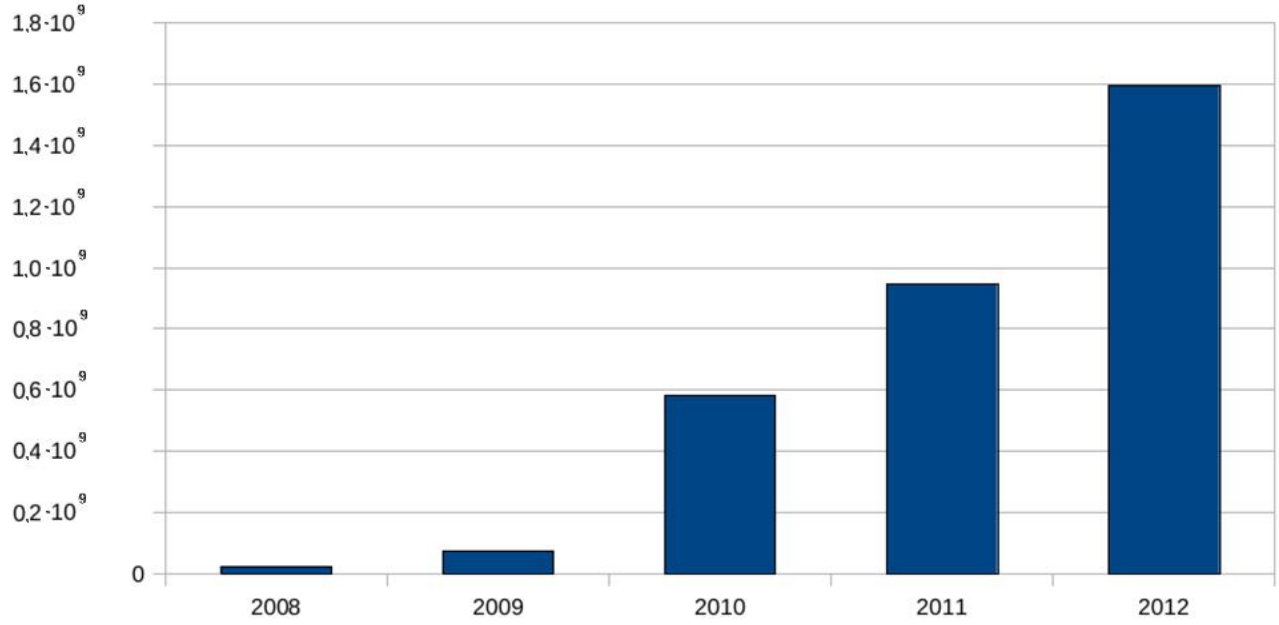


**Рис. 2.** Общее количество атак на ИС через браузер ПК
(по информации от компании "Лаборатория Касперского")

В связи с указанными выше обстоятельствами было решено разработать программное решение, предоставляющее ответственному персоналу в лице администраторов безопасности удобный инструмент, благодаря которому администратор сможет быстрее и правильнее реагировать на возникающие ситуации в компьютерной сети. Задачи, возлагаемые на программное решение, следующие:

- сбор максимально возможной статистической информации о событиях ИБ (информационной безопасности);
- хранение всех событий ИБ в удобном и быстро доступном месте для администраторов ИБ;
- выявление среди последовательности событий ИБ инцидентов ИБ;
- оповещение ответственного персонала в лице администраторов безопасности об инциденте ИБ.

В связи со спецификой задач был начат поиск и анализ подходящего математического аппарата, используя который возможно было бы описать алгоритм работы модуля анализа событий ИБ, максимально подходящий для реализации в данном программном решении. Были рассмотрены основные характеристики, достоинства и недостатки алгоритмов для анализа данных, которыми в данной задаче являются события ИБ, и дальнейшего выявления среди них атак. Набор рассматриваемых алгоритмов, подходящих по своему принципу функционирования для реализации программного решения, следующий:

- контекстный поиск на основе регулярных выражений;
- контекстный поиск на основе специальных языков;
- анализ состояния системы;

- экспертные системы;
- генетические алгоритмы;
- нейронные сети;
- статистические методы;
- иммунные системы;
- сети Петри.

В дальнейшем при анализе и сопоставлении всех достоинств и недостатков каждого алгоритма происходил выбор наиболее подходящего для данной задачи. Ниже приведены основные недостатки в решении данной задачи для каждого алгоритма:

- **Контекстный поиск на основе регулярных выражений**: в случае отсутствия конкретной сигнатуры обнаружено ничего не будет, таким образом, для двух почти одинаковых атак, одна из которых имеет соответствующую сигнатуру, а вторая нет, обнаружена будет только одна атака [12].
- **Контекстный поиск на основе специальных языков**: минусы идентичны контекстному поиску на основе регулярных выражений.
- **Анализ состояния системы**: к минусам относится малое количество параметров, характеризующих атаку, что в конечном итоге влияет на возможности описания количества состояний, являющихся нестабильными для системы [12, 13].
- **Экспертные системы**: к минусу относится то, что эти системы могут эффективно работать только в тех случаях, когда администратор безопасности может формализовать признаки проведения атаки [14].
- **Генетические алгоритмы**: невозможность работы генетического алгоритма в режиме реального времени, так как реализация данного алгоритма является очень ресурсоёмкой задачей и требует большого количества времени, что в условиях поставленной задачи при выборе алгоритма является определяющим фактором в решении не использовать данный подход. Кроме того, изложенный метод не в состоянии идентифицировать атаки с учётом последовательности возникновения событий, что также является важнейшей особенностью [12, 14].
- **Нейронные сети**: поскольку такой алгоритм всегда носит эвристический характер, то имеется большое количество ложных срабатываний, сильно влияющее на выбор метода. Процесс обучения нейронных сетей требует проведения нескольких сотен индивидуальных атак, на что требуется много времени. Также минусом является то, что функционирование происходит по принципу "черного ящика", что не позволяет объяснить процесс и логику принятия решения о факте выявления атаки при анализе произошедших событий [12, 14].
- **Статистические методы**: необходимо достаточно продолжительное время работы ИС для построения набора статистических параметров, обеспечивающего высокую эффективность выявления инцидентов ИБ. В связи с особенностью построения профилей, действует механизм динамического изменения, для более полного описания изменяющегося поведения системы [15]. Это сразу влияет на тот факт, что злоумышленник, зная об особенностях систе-

мы анализа и корреляции событий ИБ, может обмануть систему путем проведения распределенной по времени атаки, которая несущественно меняет наблюдаемые параметры. Таким образом возможно постепенно изменить режим работы, с течением какого-то времени “приручив” систему к новому поведению. Как правило, такой подход к выявлению аномалий ИБ очень часто способен выявить атаку только по последствиям, которые проявляются в виде отклонений от шаблонных значений наблюдаемых параметров [12, 15, 16].

• **Иммунные системы**: недостатки данного алгоритма в конкретной задаче полностью повторяют недостатки нейросетевого алгоритма.

Сети Петри в перечне неподходящих алгоритмов отсутствуют, так как для данной задачи они максимально подходят в силу особенностей определения многоэтапных атак ещё на промежуточных стадиях, малой ресурсоемкости и возможности определения не описанных ранее атак, за счет их аналогичности с ранее описанными.

За основу общей сводной таблицы пригодности была взята таблица в источнике [12], но в силу отсутствия актуального для данной задачи параметра она была доработана (см. табл. 2).

Таблица 2

**Сводная таблица по пригодности использования моделей**

| Характеристика / модель | Выявления известных атак | Выявления новых атак | Идентификация процесса вывода результатов работы модели | Расширяемость | Формализуемость | Простота | Масштабируемость | Время выхода на проектируемую производительность |
|---|---|---|---|---|---|---|---|---|
| Контекстный поиск на основе регулярных выражений | + | - | + | - | + | + | + | + |
| Контекстный поиск на основе специальных языков | + | - | + | + | + | + | + | + |
| Анализ состояния системы | ± | - | + | + | + | - | + | ± |
| Сети Петри | + | ± | + | + | + | - | + | + |
| Экспертные системы | ± | ± | + | + | + | - | + | ± |
| Генетические алгоритмы | ± | - | - | + | + | - | + | - |
| Нейронные сети | ± | ± | - | + | + | - | + | - |
| Статистические | ± | ± | + | + | + | + | + | ± |
| Иммунные системы | - | ± | - | + | + | - | + | - |

Таким образом, исходя из вышеизложенных данных, программное решение по анализу событий ИБ, построенное с использованием сетей Петри, будет отвечать поставленным в начале статьи задачам и обеспечивать ответственный персонал быстрым и удобным инструментом по анализу событий ИБ на всех компьютерах сети.

## Литература


1. ***InfoWatch,*** Глобальное исследование утечек 2008, 2009 // http://www.infowatch.ru/analytics/reports/143.
2. ***InfoWatch,*** Глобальное исследование утечек 2009, 2010 // http://www.infowatch.ru/analytics/reports/141.
3. ***InfoWatch,*** Глобальное исследование утечек 2010, 2011 // http://www.infowatch.ru/analytics/reports/462.
4. ***InfoWatch,*** Глобальное исследование утечек 2011, 2012 // http://www.infowatch.ru/analytics/reports/2583.
5. ***InfoWatch,*** Глобальное исследование утечек 2012, 2013 // http://www.infowatch.ru/analytics/reports/3011.
6. **Symantec** Global Internet Security Threat Report, Trends for 2009, Volume XV, 2010.
7. ***Virus*** Definitions & Security Updates // http://www.symantec.com/business/security_response/definitions.jsp.
8. ***Triumfant,*** The Worldwide Malware Signature Counter // http://www.triumfant.com/Signature_Counter.asp.
9. ***Kaspersky*** Security Bulletin. Основная статистика за 2010 год, 2011 // http://www.securelist.com/ru/downloads/vlpdfs/k_securitybulletin_rus2_screen.pdf.
10. ***Kaspersky*** Security Bulletin. Основная статистика за 2011 год, 2012 // http://www.securelist.com/ru/analysis/208050741/Kaspersky_Security_Bulletin_Osnovnaya_statistika_za_2011_god.
11. ***Kaspersky*** Security Bulletin. Основная статистика за 2012 год, 2012 // http://www.securelist.com/ru/analysis/208050778/Kaspersky_Security_Bulletin_2012_Osnovnaya_statistika_za_2012_god.
12. ***Сердюк В.А.*** Новое в защите от взлома корпоративных систем. М.: Техносфера, 2007. 360с.
13. ***Сундеев П.В.*** Функциональная стабильность критичных информационных систем: основы анализа // Научный журнал КубГАУ. № 7 (05). 2004.
14. ***Рассел С., Норвиг П.*** Искусственный интеллект: современный подход, 2-е изд., М.: Вильямс, 2007. 1408 с.
15. ***Аграновский А.В., Хади Р.А.*** Системы обнаружения компьютерных угроз // Сетевые решения. № 5. 2008. http://www.nestor.minsk.by/sr.
16. ***Аграновский А.В., Хади Р.А.*** Новый подход к защите информации – системы обнаружения компьютерных угроз // Информационный бюллетень Jet Info, № 4 (167). 2007. 24 с.