Половко Иван Юрьевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: i.y.polovko@gmail.com; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; к.т.н.; ассистент.

Polovko Ivan Yur'evich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: i.y.polovko@gmail.com; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security of information technologies; cand. of eng. sc.; assistant professor.

УДК 004.056.5, 004.89

А.В. Никишова, А.Е. Чурилина

ОБНАРУЖЕНИЕ РАСПРЕДЕЛЕННЫХ АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ ПРЕДПРИЯТИЯ

Современный этап развития информационных систем основан на достижениях телекоммуникационных технологий, что обуславливает применение распределенной обработки информации. Это привело к появлению нового вида атак на информационные системы, распределенных как во времени, так и в пространстве.

По данным Лаборатории Касперского в период 2013 г. были распространены целевые атаки, использующие разнообразные средства проникновения. Также зафиксировано большое количество взломов корпоративных сетей. Подобные атаки характеризуются большой сложностью и имеют многошаговый алгоритм действий и распределенный характер [1].

Предложена многоагентная система обнаружения атак (СОА), использующая предположение о многошаговости реализации атак на информационные системы предприятий, что подтверждается приведенной статистикой. Система использует адаптивный метод обнаружения атак – нейронные сети.

Эксперименты показали, что предложенный подход для построения многоагентной СОА позволяет уменьшить вероятность ложного срабатывания используемого адаптивного метода обнаружения атак при неувеличении вероятности пропуска атаки.

Атака; распределенные атаки; система обнаружения атак; многоагентная система обнаружения атак; интеллектуальный агент; нейронная сеть.

A.V. Nikishova, A.E. Churilina

DISTRIBUTED INTRUSION INTO INFORMATION SYSTEM OF ENTERPRISE DETECTION

Modern phase of information systems' development is based on the achievements of telecommunication technologies that causes the application of distributed information processing. This led to the emergence of a new type of intrusion into information systems, distributed in both time and space.

According to Kaspersky Lab in the period 2013 targeted intrusions were distributed using a variety of means of penetration. Also large number of corporate networks' hacks was recorded. These intrusions are characterized by great complexity and have a multi-step algorithm of actions and distributed nature [1].

Multi-agent intrusion detection system (IDS) that uses the assumption of multi-step of intrusions into enterprises' information systems implementation, which is confirmed by the given statistics, is suggested. The system uses the adaptive method of intrusion detection – neural networks.

Experiments showed that the suggested approach for building multi-agent IDS allows reducing the risk of used adaptive intrusion detection method false positives when not increasing the probability of intrusion missing.

Intrusion; distributed intrusion; intrusion detection system; multi-agent intrusion detection system; intelligent agent; neural network.

Статистика организаций, работающих в области защиты информации, например, McAfee Inc, показывает относительно стабильный рост количества новых образцов атакующих воздействий (рис. 1) [2].

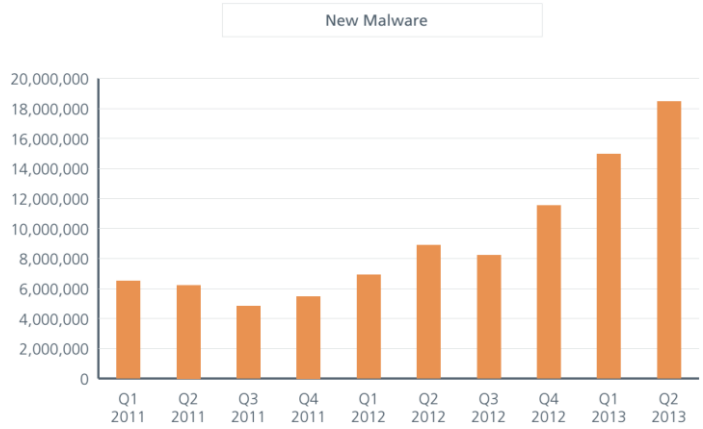

Рис. 1. Количество новых образцов атакующих воздействий по кварталам

Постоянно возникающие новые виды атак обуславливают необходимость применения адаптивных методов для обнаружения атак, позволяющих уменьшить вероятность пропуска атак, например, статистических методов [3], нейронных сетей [4], иммунных сетей [5]. Однако подобные методы обладают большой вероятность ложных срабатываний, что ограничивает их широкое применение. А потому целью предлагаемой многоагентной СОА является снижение вероятности ложных срабатываний при неувеличении вероятности пропуска атак.

По результатам анализа типовых информационных систем предприятия [6] и основных злоумышленных воздействий на них [7], была предложена архитектура многоагентной СОА (рис. 2).

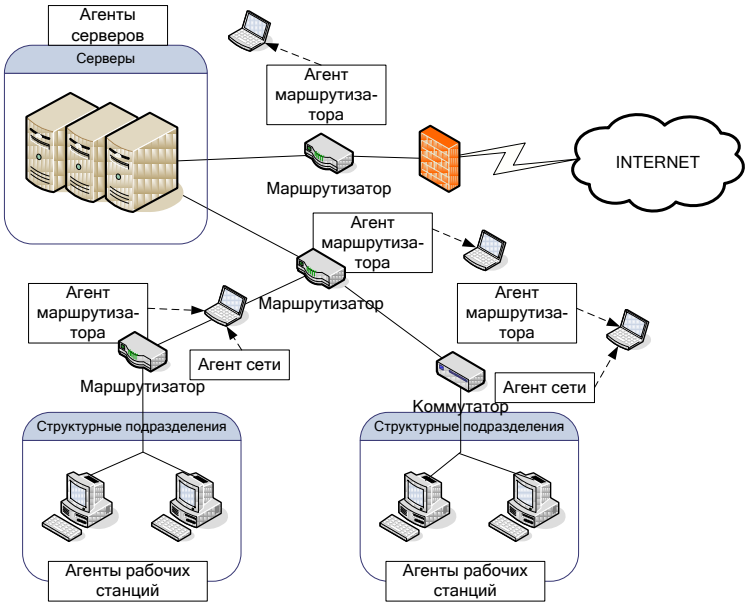

Рис. 2. Архитектура многоагентной СОА

Многоагентная СОА имеет вид $MAS = \{A_R, A_N, A_S, A_W\}$, где

$A_R = \{A_R^v, A_R^o\}$ – множество агентов маршрутизаторов, делится на подмножество агентов внешних маршрутизаторов A_R^o и подмножество агентов внутренних A_R^v маршрутизаторов;

A_N – множество агентов сети, анализирующие сведения о пакетах, передаваемых по сети, N. Данный агент располагается в каждом сегменте сети;

$A_S = \{A_S^1, ..., A_S^n\}$ – множество агентов серверов. На каждом сервере располагаются несколько агентов различных типов A_S^i, где i=1..n – зависит от функционального назначения сервера, которые анализируют события, наиболее критичные с точки зрения безопасности;

$A_W = \{A_W^1, ..., A_W^m\}$ – множество агентов рабочих станций. На каждой рабочей станции располагается несколько агентов различных типов A_W^j, где j=1..m – зависит от функционального назначения рабочей станции, которые проводят анализ событий, наиболее критичных с точки зрения безопасности.

Каждый агент имеет структуру, содержащую выбранный адаптивный метод обнаружения атак – нейронную сеть, и описывается состоянием (P, B, S, G, I), где

P – ощущение. Представляет собой информацию об окружающей среде, собираемую агентом, т.е. набор входных данных агента, различается в зависимости от типа агента.

B – убеждения. Множество убеждений, т.е. сведений и знаний об окружающей агента среде. Убеждения агента представляют собой нейронную сеть. На первом этапе агенты собирают сведения о нормальном функционировании информационной системы, злоумышленных действиях, нарушениях политики безопасности и т.д., и на основе них создают обучающую выборку для нейронной сети.

S – ситуация. Конкретное состояние среды, т.е. конкретные значения входных данных и результата классификации их нейронной сетью.

G – цели. Определяется как желаемое состояние среды.

I – намерения. Множество возможных планов действий агента.

Для реализации предложенной структуры агентов была разработана архитектура программной реализации агента (рис. 3).

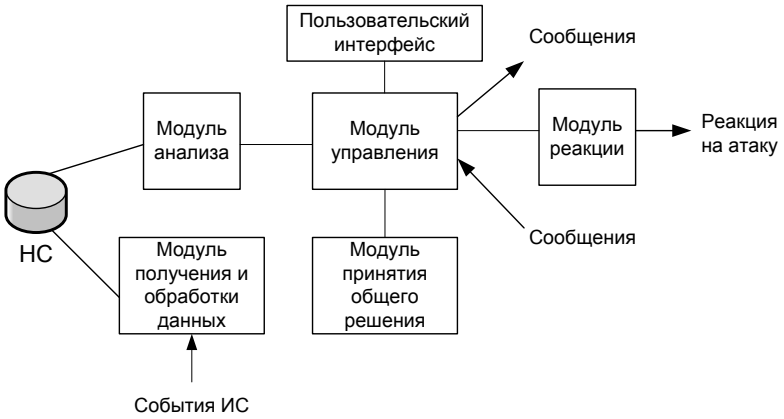

Рис. 3. Архитектура агента

Модуль управления осуществляет получение настроек из пользовательского интерфейса и передачу результатов анализа сведений о состоянии информационной системы агентом на пользовательский интерфейс. Также он производит аутентификацию субъекта взаимодействия, общую настройку агента, запуск процесса анализа и процесса принятия общего решения, передачу данных и инициацию процесса генерации и интерпретации сообщений, управляет реакцией агента.

Модуль получения и обработки данных получает данные из определенного источника сведений о состоянии информационной системы, проводит их преобразование в вид, необходимый для передачи на вход нейронной сети. Полученные данные передаются на вход нейронной сети и записываются в базу данных – обучающую выборку.

Модуль анализа, получив результат анализа от нейронной сети, записывает выход нейронной сети в базу данных и интерпретирует его. В зависимости от значения выхода событие либо игнорируется, либо управление передается на модуль управления для инициации принятия общего решения агентами, либо управление передается модулю управления для формирования реакции агента на атаку.

Модуль реакции осуществляет выполнение намерений агента. В зависимости от типа агента и настроек, агент может сообщить сведения об атаке специалисту по защите информации, отправить ICMP-пакет, сообщающий атакующему узлу о недоступности узла, сети или сервиса, или приостановить или завершить процесс.

В случае если выход нейронной сети агента не позволяет однозначно отнести анализируемое событие к нормальному поведению компонента информационной системы или к атакующему воздействию, вызывается модуль принятия решения [8]. Он формирует упорядоченные предпочтения агента и инструктирует модуль управления сгенерировать и отправить сообщения своим соседям об инициации процедуры принятия общего решения. После получения наборов упорядоченных предпочтений, модуль проводит процедуру голосования. В случае если совместное решение показало ошибку агента, запускается таймер. По истечению времени таймера процедура повторяется снова, но не более n раз. Если после повторений процедуры, будет подтверждена ошибка агента, уменьшается его показатель качества. При достижении показателем качества порогового значения, убеждения агента пересматриваются.

Эксперименты проводились на фрагменте сети, состоящей из сервера, двух маршрутизаторов, двух подсетей и 4 рабочих станций. Были установлены 4 агента рабочей станции, 2 агента сети, 2 агента маршрутизатора и 1 агент сервера.

В обучающую выборку для нейронных сетей агентов к нормальным событиям информационной системы случайным образом, согласно нормальному закону распределения, были добавлены:

- образцы атакующих воздействий;
- нарушение политики безопасности;
- образцы аномального поведения компонентов информационной системы.

В ходе экспериментов было сделано предположение о многошаговости и распределенности атакующих воздействий. На основании этого в случае неспособности нейронной сети отнести анализируемое событие к нормальному поведению компонента информационной системы или атакующему воздействию, все одиночные события рассматривались как штатное отклонение от функционирования информационной системы и игнорировались, группы подобных событий расценивались как атакующие воздействия, что вызывало реакцию со стороны многоагентной СОА.

При этом в тестовую выборку были включены сетевые пакеты вида, представленного в табл. 1, не входящие в обучающую выборку, т.е. являющиеся аномальными для функционирования ИС.

Таблица 1

Фрагмент тестовой выборки

IP источника	IP получателя	Порт источника	Порт получателя	Идентификатор	Протокол	TCP флаги	ICMP тип
3232249857	3232249860	49160	445	34816	6	24	-1
3232249860	3232249857	445	49160	136	6	24	-1

При перехвате аномальных пакетов от рабочей станции 1 к рабочей станции 3 агент сети 1 классифицирует пакет 3-м уровнем опасности (рис. 4).

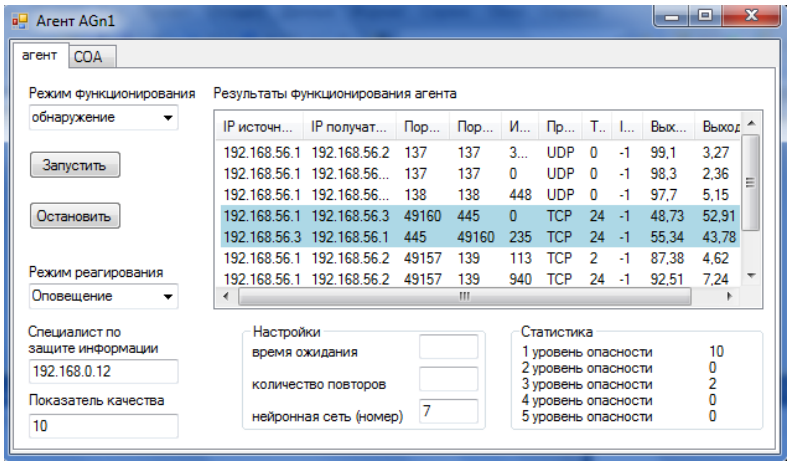

Рис. 4. Результат классификации пакета агентом сети 1 (экранная копия)

Агент инициирует принятия общего решения. В принятии общего решения учувствуют агенты рабочих станций 1 и 3, текущий уровень опасности у которых равен 1 (рис. 5) и их предпочтения равны 12345; агент маршрутизатора 2, текущий уровень опасности у которого равен 1 и предпочтения равны 12345; и агенты сети 1 и 2, текущий уровень опасности которых равен 3 и их предпочтения равны 34251.

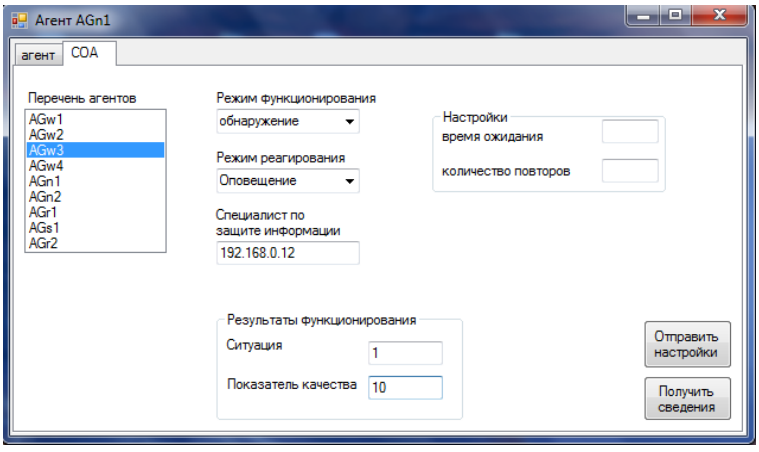

Рис. 5. Текущая ситуация агента рабочей станции 3 (экранная копия)

В результате принятия общего решения, уровень опасности для информационной системы был определен как 1-ый, значение выходов нейронных сетей агента сети 1 и 2 было заменено на середину интервала выбранного уровня опасности, их показатель качества был уменьшен (рис. 6).

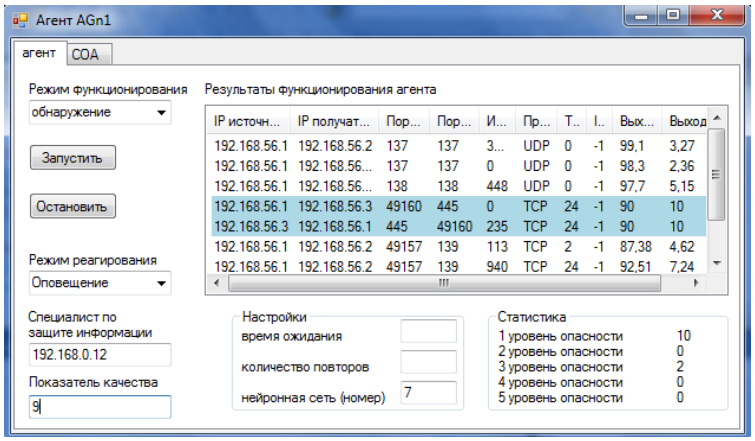

Рис. 6. Пересмотр убеждений агента сети 1 (экранная копия)

После этого в тестовую выборку также были включены события рабочих станций вида, представленного в табл. 2, не входящими в обучающую выборку.

Таблица 2

Фрагмент тестовой выборки

Событие	Тип	Пользователь	Время
4783	4	1013	30180
4722	5	1013	29703
4688	4	1113	33280
4689	4	1113	46400
4624	4	1013	77421
4702	4	1013	77425

Агент рабочей станции 3 классифицирует подобные аномальные события 4-м уровнем опасности (рис. 7).

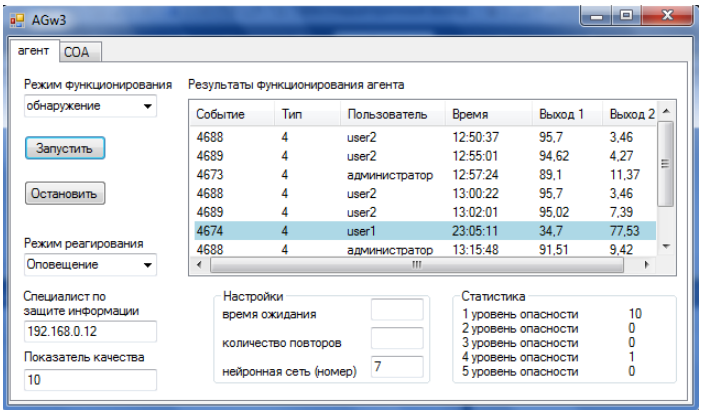

Рис. 7. Результат классификации пакета агентом рабочей станции 3 (экранная копия)

В принятии общего решения учувствуют агент рабочей станции 1, текущий уровень опасности у которого равен 1 и его предпочтения равны 12345; агент рабочей станции 3, текущий уровень опасности у которого равен 4 и его предпочтения равны 45321; агент маршрутизатора 2, текущий уровень опасности у которого равен 1 и предпочтения равны 12345; агенты сети 1 и 2, текущий уровень опасности которых равен 3 и их предпочтения равны 34251.

В результате принятия общего решения уровень опасности для информационной системы был определен как 3-ий, и было отправлено извещение специалисту по защите информации (рис. 8).

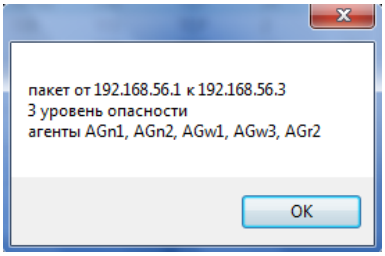

Рис. 8. Оповещение специалиста по защите информации (экранная копия)

В экспериментах показана эффективность применения процедуры принятия общего решения.

Было сгенерировано 250 одиночных аномальных событий, 250 групп аномальных событий ИС. Эти события случайным образом в соответствии с нормальным законом распределения были встроены в поток нормальных событий информационной системы, общее количество которых составило 50000. Было проведено 100 испытаний. Средние значения испытаний представлены в табл. 3.

Таблица 3

Результаты экспериментов

	Без применения алгоритма принятия общего решения	С применением алгоритма принятия общего решения
Число нормальных событий	50000	50000
Количество событий, определенных как атака	617	346
Количество пропусков атаки	11	10
Количество ложных срабатываний	384	101

На основании данных из таблицы 3 вероятность ошибки 1-го рода – пропусков атаки, в первом случае составила 0,044, а во втором случае – 0,040.

Вероятность ошибки 2-го рода – ложных срабатываний, в первом случае составила 0,0076, а во втором случае – 0,0020.

В среднем вероятность ошибки 1-го рода уменьшилась в 1,1 раз, а вероятность ошибки 2-го рода уменьшилась в 3,8 раза.

Под эффективность предложенной многоагентной СОА будем понимать свойство системы получать требуемый результат ее функционирования, т.е. обнаружение атак, соотнесенное с затратами ресурсов [9]. Тогда показатель эффективности рассчитывается по формуле:

$$E = \frac{A}{R},$$

где E – показатель эффективности, A – потенциальный эффект, R – ресурсоемкость.

В качестве потенциального эффекта принимается количество ошибок 1-го и 2-го рода. А в качестве ресурсоемкости – количество событий, обрабатываемых многоагентной СОА в секунду.

По результатам экспериментов показатель эффективности E_1 многоагентной СОА, функционирующей без применения алгоритма принятия общего решения, составил:

$$E_1 = \frac{389}{5476} = 0.07$$

Показатель эффективности E_2 многоагентной СОА, функционирующей с применением алгоритма принятия общего решения, составил:

$$E_2 = \frac{122}{5459} = 0.02$$

При расчете полагалось, что принятие общего решения, состоящее из трех циклов расчетов, осуществлялось один раз в секунду.

В связи с особенностями выбора показателей, чем меньшее значение имеет показатель эффективности, тем эффективнее СОА. Расчеты показали повышение эффективности в 3,5 раза при применении многоагентной СОА с применением алгоритма принятия общего решения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Масленников Д.* Развитие информационных угроз в первом квартале 2013 года [Электронный ресурс] // Лаборатория Касперского. Аналитика от 15 мая 2013 г. URL: http:// www.securelist.com / ru / analysis / 208050801 / Razvitie_ informatsionnykh_ugroz_v_ pervom_kvartale_2013_goda (дата обращения: 15.10.2013).
2. McAfee Threats Report: Second Quarter 2013 [Электронный ресурс] // McAfee Labs. Reports. URL: http://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q2-2013.pdf.
3. *Будько М.Б., Будько М.Ю.* Отслеживание изменений в структуре сети и решение задач повышения безопасности на основе анализа потоков данных // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2009. – № 59. – С. 78-82.
4. *Абрамов Е.С., Сидоров И.Д.* Метод обнаружения распределенных информационных воздействий на основе гибридной нейронной сети // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 154-164
5. *Аткина В.С.* Применение иммунной сети для анализа катастрофоустойчивости информационных систем // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 203-210.
6. *Никишова А.В.* Архитектура типовой информационной системы для задачи обнаружения атак // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 104-109.
7. *Максимова Е.А., Корнева В.А.* Формализация действий злоумышленника при прогнозировании вторжений в корпоративную информационную систему // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы II Всероссийской науч.-практ. конф., г. Волгоград, 26 апреля 2013 г. – Волгоград: Изд-во ВолГУ, 2013. – С. 71-78.
8. *Никишова А.В.* Кооперация агентов многоагентной системы обнаружения атак // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы II Всероссийской науч.-практ. конф., г. Волгоград, 26 апреля 2013 г. – Волгоград: Изд-во ВолГУ, 2013. – С. 118-120.

9. *Максимова Е.А., Корнева В.А.* Оптимизация технологии безопасного информационного взаимодействия в корпоративных системах // Материалы XII Международной научно-практической конференции «ИБ-2012». Ч. II. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 124-129.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Никишова Арина Валерьевна – Волгоградский государственный университет; e-mail: arinanv@mail.ru; 400062, г. Волгоград, пр. Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; старший преподаватель.

Чурилина Александра Евгеньевна – e-mail: sashune4ka-ch@mail.ru; кафедра информационной безопасности; ассистент.

Nikishova Arina Valerievna – Volgograd State University; e-mail: arinanv@mail.ru; 100, Universitetsky pr., Volgograd, Russia, 400062; phone: +78442460368; the department of informational security; senior lecturer.

Churilina Aleksandra Eugenievna – e-mail: sashune4ka-ch@mail.ru; the department of informational security; assistant professor.

УДК 004.052.2

А.М. Максимов

АНАЛИЗ ОСОБЕННОСТЕЙ ОСУЩЕСТВЛЕНИЯ АТАК НА ВЕБ-СЕРВЕР ПОСРЕДСТВОМ ГЕНЕРАЦИИ ОШИБОЧНЫХ ЗАПРОСОВ

Статья посвящена рассмотрению особенностей функционирования веб-сервера Microsoft IIS. Рассматриваются условия, когда результатом на запросы к веб-ресурсу (умышленные или неумышленные) вместо действительной информации происходит выдача кодов ошибок (например, ошибки класса 4xx, которые являются кодами состояния HTTP). В результате таких запросов может происходить повышение потребления ресурсов веб-сервером, что при достижении некоторых установленных предельных лимитах может стать причиной отказа в обслуживании веб-сервером, или его сильного замедления обработки новых поступающих запросов.

Помимо описания проблемы в статье приводятся некоторые данные проведённых тестов, условия, в которых были получены результаты. Также указываются параметры, которые необходимо учитывать при вынесении прогнозов и оценок конечного результата. По результатам рассмотрения выявленных данных предлагаются некоторые методы, которые могут помочь сгладить негативные результаты запросов, вызывающих выдачу ошибок вместо действительного результата. Не оставлены без рассмотрения и негативные аспекты, которые могут быть следствием предлагаемых методов, и которым следует уделить внимание для того чтобы они не оказали существенного отрицательного влияния на конечный результат.

Веб-сервер; код состояния HTTP; нагрузка; отказ в обслуживании; IIS; HTTP.

A.M. Maximov

ANALYSIS OF ATTACK FEATURES TO WEB SERVER THROUGH REQUESTS WITH ERRORS

The article contains review of functioning features of Microsoft IIS web server under conditions when errors occur (error class 4xx, which are HTTP status codes in fact, for example) as result of requests (intentional or unintentional) instead of actual information. Increased resource usage may occur as result of these requests with errors, so if preset limits are reached, it can be a cause of web server denial of service or significant delays in processing of requests of all type (even actual, without evil intent).