Pashchenko Ivan Nikolaevich – Ufa State Aviation Technical University; e-mail: iv.pashchenko@gmail.com; 12, K. Marxa street, Ufa, 450000, Russia; phone: +73472730672; the department of computer science and information security; postgraduate student.

Vasyliev Vladimir Ivanovich – e-mail: vasilyev@ugatu.ac.ru; the department of computer science and information security; head the department; dr. of eng. sc.; professor.

УДК 004.056

И.Ю. Половко

РАЗРАБОТКА ТРЕБОВАНИЙ К СОСТАВУ ХАРАКТЕРИСТИК ДЛЯ СРАВНЕНИЯ СОА*

Работа посвящена актуальной проблеме выбора средства защиты, для обеспечения надежной работы компьютерной сети. В качестве средства защиты рассматривается система обнаружения атак (СОА). Обоснована необходимость выработки требований к составу качественных характеристик СОА, позволяющих получить взвешенную оценку качества исследуемых систем.

Показано, что характеристики структурно делятся на две группы – для оценки функциональных свойств системы и для оценки производительности. Обоснован выбор данных характеристик. При разработке характеристик оценки качества СОА исследовались, в первую очередь, те механизмы СОА, которые наиболее критичны для атак, а значит, могут повлиять на эффективность обнаружения атак. Выявлены наиболее уязвимые аспекты в работе СОА при обнаружении атак. Для этого был рассмотрен подход, основанный на исследовании слабых сторон протоколов, использование которых позволяет легально обойти механизмы СОА. Таким образом, показано, что СОА, чётко следующие RFC, оказываются уязвимыми. Разработанные характеристики позволяют оценить степени соответствия реальных и заявленных производителем функциональных свойств СОА.

Сетевая безопасность; СОА; характеристики качества; критерии оценки.

I.Yu. Polovko

THE DEVELOPMENT OF REQUIREMENTS TO THE CHARACTERISTICS OF NIDS FOR COMPARISON

The scientific work is devoted to the actual problem of selecting protection to provide reliable operation of the network. As a means of protection consider the intrusion detection system (NIDS). The necessity of developing requirements to the structure of quality characteristics of NIDS, was justified. That allowing to obtain a balanced quality assessment of the systems.

The characteristics structurally divided into two groups – to evaluate the functional properties of the system and for performance evaluation. The choice of, these characteristics was justified. Primarily was investigated mechanisms of NIDS, during the development of characteristics of the NIDS, that are most critical for the attack, thus may affect on efficiency of detection of attacks. Has been identified the most vulnerable aspects of NIDS at the detection of attacks. For this was considered an approach based on a study of the weaknesses of protocols, the using of which allows you to legally circumvent the mechanisms of NIDS. That is shown that the NIDS that are clearly following RFC, are vulnerable. The developed characteristics allows to estimate the compliance of the real and the manufacturer's functional properties of NIDS.

Network security; NIDS; quality characteristics; evaluation criteria.

* Работа выполнена при поддержке гранта РФФИ № 12-07-00014-а.

На сегодняшний день, на рынке информационных услуг представлено множество различных средств защиты компьютерной сети, и данный перечень регулярно пополняется новыми продуктами. Какое средство защиты выбрать пользователю, чтобы оно максимально точно отвечала установленным требованиям, становится весьма не просто.

Данная статья посвящена одному из ключевых компонентов защиты компьютерной сети, а именно Системе обнаружения атак, и описывает механизм выбора необходимого продукта, который будет максимально отвечать требованиям пользователя.

Стандартизированного подхода к оценке качества СОА, на сегодняшний день, не существует. Тесты, которые предлагают производители, обладают маркетинговой направленность и не позволяют оценить функциональные возможности различных систем, чтобы впоследствии сравнить их и сделать обоснованный выбор.

Термин «СОА» – Системы обнаружения компьютерных атак (IDS – Intrusion Detection Systems) – один из важнейших элементов систем информационной безопасности компьютерных сетей. СОА представляет собой программное или аппаратное средство, служащее для выявления фактов неавторизованного доступа в компьютерную систему или сеть.

Качество СОА – это совокупность характеристик СОА, обуславливающих её способность удовлетворять определенным требованиям в соответствии с назначением. Сам термин «характеристики» определяет объективные стороны объекта, без оценивания важности самих характеристик для потребителя. Оценка качества работы СОА включает в себя рассмотрение ее количественных и качественных характеристик. Другими словами, оценивается производительность СОА и ее функциональные возможности.

Основные значимые компоненты СОА. Рассмотрим модель СОА, предложенную CIDF [1], которая включает в себя четыре основных компонента:

1. Генератор событий (e-box, event) – собирает данные для принятия решения анализатором. Данные могут содержать имя контролируемого параметра, его особенности и значения.
2. Анализатор (a-box, analyzer) – принимает решение о наличии симптомов атаки на основании данных от сенсоров. Анализатор может выполнять функции преобразования, фильтрации, нормализации и корреляции данных.
3. Хранилище данных (d-box, database) – необходимо для принятия решения и хранения данных сенсоров. Кроме того, в хранилище содержатся параметры управления (перечни контролируемых параметров, частота проведения контроля и т.д.) и семантические описания атак.
4. Модуль реакции системы на обнаруженную атаку (r-box, reaction) – при пассивной реакции система обнаружения вторжений оповещает администратора о начале атаки, используя выдачу сообщения на экран монитора, посылку e-mail, сигнал на пейджер или звонок на сотовый телефон. Схема взаимодействия основных компонентов модели CIDF приведена на рис. 1.

Область действия качественных характеристик. Качественные характеристики (функциональные) – представляют собой набор критериев для оценки работоспособности СОА в типовой окружающей среде, когда атакующий находится вне сети, в которой расположена СОА, например, в Internet.

Определение функциональных возможности СОА (например, способности обнаруживать атаки, сообщать об инцидентах, сохранять информацию), является основной задачей характеристик качества. Они позволяют наиболее полно выявить недостатки тестируемой системы обнаружения атак.

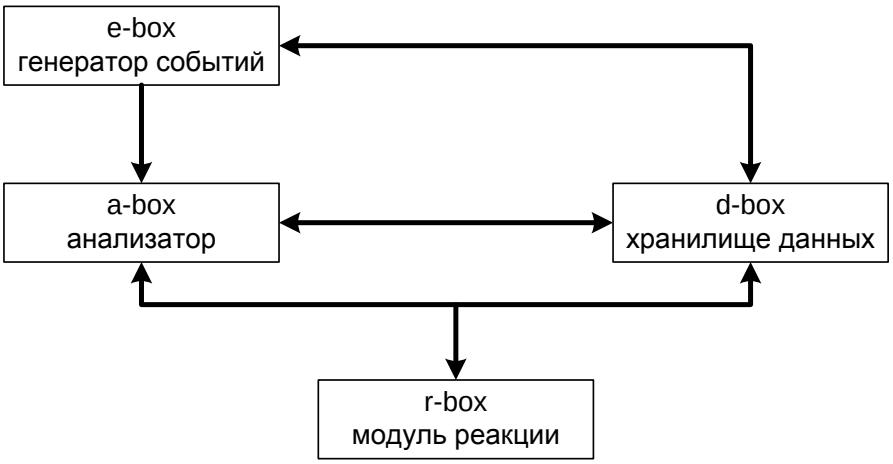

Рис. 1. Схема взаимодействия основных компонентов модели CIDF

Механизм выбора характеристик качества

При разработке требований к набору функциональных характеристик для оценки качества СОА исследуются функции, которые могут повлиять на эффективность обнаружения атак:

- функции, наиболее критичные для собственно обнаружения атак;
- функции, критичные для противостояния тем атакам, приоритетной целью которых являются непосредственно СОА [2].

Для получения ответа на вопрос о наиболее критичных аспектах работы СОА при обнаружении атак, используется следующий подход. При разработке СОА, в неё закладываются знания о функционировании протоколов стека TCP/IP. Этот подход обращает внимание на слабые стороны протоколов, использование которых позволяет легально обойти механизмы СОА. Таким образом, СОА, основанная на следовании RFC, оказывается уязвимой вне зависимости от точности следования.

Уязвимости систем обнаружения атак. Системы обнаружения атак имеют свои слабые стороны и уязвимости. Рассмотрим основные уязвимости сетевых СОА и методы, которые могут использовать злоумышленники для ее обмана.

Каждый из компонентов СОА, указанных в модели CIDF, имеет свое уникальное назначение и может быть атакован по разным причинам.

Атаки против e-box, работающие с входными «сырыми» (raw) данными, позволяют блокировать реальные события, происходящие в контролируемой системе. Атака против e-box сетевой СОА может сделать недоступным получение пакетов из сети или сделать недоступным соответствующее декодирование этих пакетов.

Некоторые СОА используют сложный анализ. В таких системах надежность используемого a-box очень важна, поскольку атакующий может обойти систему обнаружения. Кроме того, сложная техника обнаружения может предоставить различные пути для проведения атаки. С другой стороны, простейшие системы могут пропустить атаки, в которых злоумышленник маскирует свою деятельность сложным скоординированным взаимодействием или взаимосвязями.

Злоумышленник может разрушить компоненты d-box, чтобы защититься от записи деталей атаки. Неправильно используемая БД может позволить ему, произвести замену или удаление зарегистрированных данных об атаке. Данные сценарии необходимо учитывать при создании надежной базы данных.

Слабой стороной сетевых СОА является то, что они принимают решение на основе анализа сетевого трафика, поэтому не могут предвидеть, как поведет себя целевая система при получении этого трафика [3]. Также необходимо учитывать, что сами СОА могут быть подвержены атакам отказа в обслуживании (выведение их из строя или исчерпание их ресурсов).

Сетевые СОА функционируют как пассивные устройства, обнаруживающие аномалии и злоупотребления (сигнатуры). Методы обнаружения аномалий для сетевых СОА используются довольно редко, из-за большого числа ложных срабатываний и потребности в большом периоде времени для построения «нормального» поведения. Основные методы обхода СОА, работающих на обнаружение злоупотреблений:

- сбивание с толку;
- фрагментация;
- шифрование;
- перегрузка.

Примеры техники обхода сетевых СОА.

Фрагментация – это процесс разделения пакетов на множество фрагментов. Данная процедура применяется, когда пакет слишком большой для передачи по сети. Это может происходить на любом роутере (если не установлены запрещающие флаги). Принимающая система хранит поступающие фрагменты, выделяет ресурсы для ожидания ещё не принятых и собирает их в правильном порядке. Что бы проходить через роутер, TTL фрагментов должно быть больше 1, так как роутер уменьшает TTL полученного пакета на единицу. Если TTL фрагмента равно 1, оно станет равным 0, и пакет не пойдет дальше, а будет отброшен. Отправителю в этом случае будет отправлено ICMP сообщение: "Time Exceeded In Transit".

Таймаут сборки фрагментов (IP Fragment Reassembly Timeout) указывает время, которое фрагмент будет храниться несобранным. По истечению таймаута фрагмент будет отброшен. В различных ОС это значение имеет разную величину и может быть использовано для определения версии системы. СОА так же реассемблируют фрагменты и имеют такой же таймаут. Для примера, в СОА Snort по умолчанию значение таймаута равно 60 секунд, после истечения которых, пакет с первым фрагментом уничтожается и соединение сбрасывается.

Если реассемблировать фрагменты в отведенное время невозможно, хост или роутер должен выслать сообщение об истечении времени сборки пакета (ICMP Fragment Reassembly Time Exceeded message, ICMP type=11, code=1), как регламентируется в RFC-792. Сообщение посылать не требуется, если первый фрагмент потока недоступен [2].

1. Таймаут СОА меньше времени сборки у целевой системы.

Предположим, что на СОА значение таймаута сборки составляет 15 секунд, а на целевой системе (цели атаки, защищаемой системе) – 30 секунд (время, установленное по умолчанию для Linux). Тогда после посылки первого фрагмента, злоумышленник может послать новый первый фрагмент, с другим содержимым, в промежутке от 15 до 30 секунд, как это происходит показано на рис. 2.

В этом случае СОА будет отбрасывать первый пакет из-за превышения таймаута сборки (и не принимать второй), а на целевой машине поток будет собираться правильно. В результате атака может достигнуть цели, при этом тревога поднята не будет.

2. Таймаут СОА больше чем у жертвы.

У ОС Linux/FreeBSD таймаут сборки по умолчанию составляет 30 секунд, а у Snort – 60. Схема использования этой техники обхода показана на рис. 3. Нарушитель делит пакет на четыре сегмента с номерами 1, 2, 3, 4 соответственно.

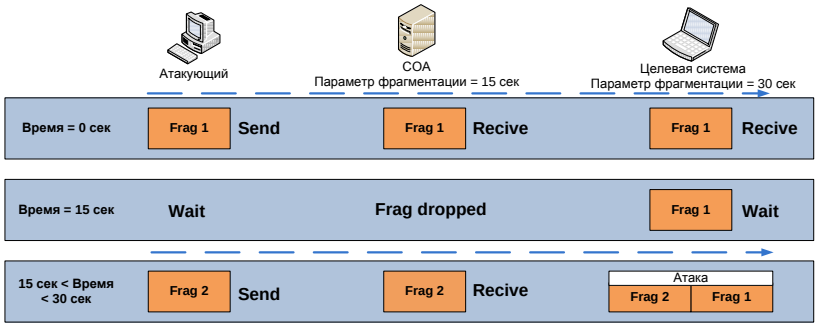

Рис. 2. Обход с использованием техники таймаута сборки (1)

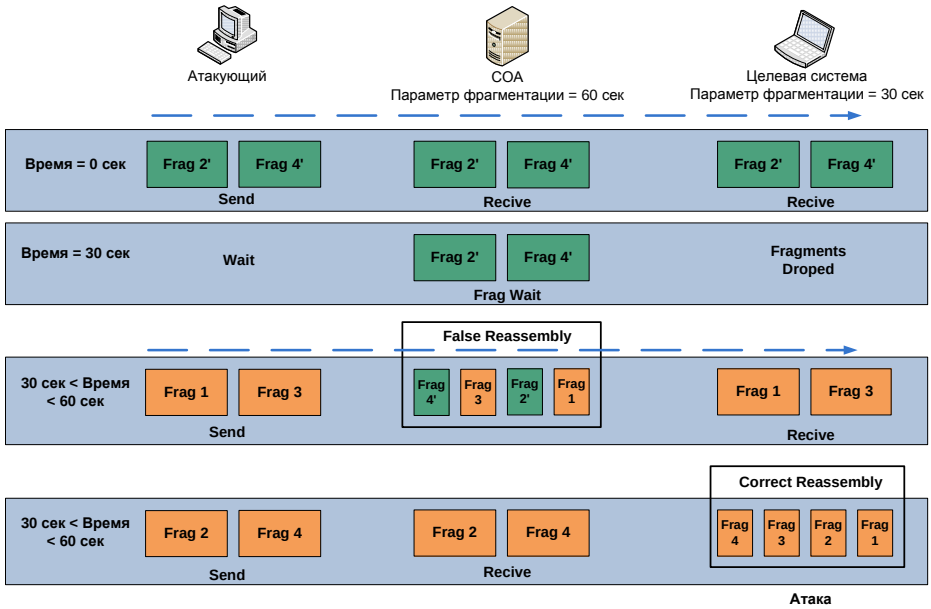

Рис. 3. Обход с использованием техники таймаута сборки (2)

В первом случае фрагменты 2 и 4 не содержат никакой полезной информации (обозначим их 2' и 4'). Они получаются и целевой системой, и СОА. Нарушитель должен дождаться, пока фрагменты на целевом компьютере будут отброшены. Тогда у целевого компьютера нет первого фрагмента и, соответственно, ICMP сообщение об истечении времени сборки не будет отправлено. После сброса злоумышленник сначала посылает новые пакеты (с номерами 1 и 3) с нужной ему информацией, затем пакеты с номерами 2 и 4, но уже с нужной ему информацией. Система обнаружения атак уже реассемблировала сессию со старыми фрагментами, поэтому новые пакеты 2 и 4 дойдут до цели. В результате целевая система получит все 4 части с правильной информацией, а СОА только две, и не сможет зарегистрировать атаку.

3. Атака на систему обнаружения атак с использованием TTL

В этом случае атакующему необходимо точно знать, сколько роутеров на маршруте между ним и целевой системой, что можно установить, воспользовавшись утилитой traceroute (рис. 4).

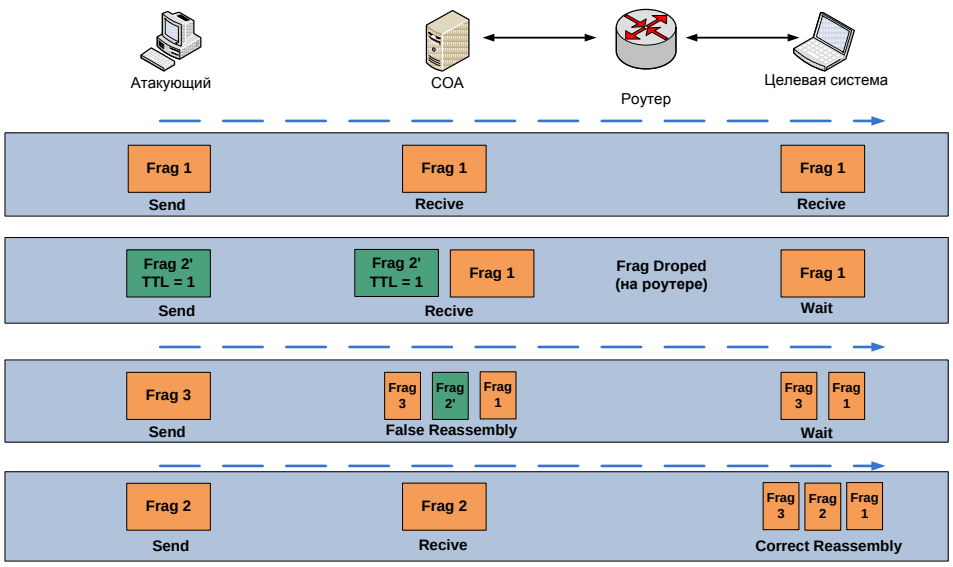

Рис. 4. Атака COA с использованием TTL

Между COA и целевой системой расположен роутер. Нарушитель разбивает атаку на три фрагмента. Первый фрагмент имеет большое значение TTL и будет получен как целевым компьютером, так и COA. Второй фрагмент (обозначенный 2') является «мусорным» и его TTL равно 1. Он будет получен COA, но на роутере будет отброшен, поскольку его TTL станет равным 0. После этого посылается третий фрагмент с правильным TTL. COA соберёт все фрагменты и проверит их, а целевая система будет ожидать средний фрагмент. Когда после этого злоумышленник отправит второй пакет с нужной информацией и правильным TTL, он будет проигнорирован COA. Целевая система сможет собрать весь поток, и атака будет завершена.

4. Политики сборки пакетов

В существующих ОС сборка фрагментов осуществляется разными способами [4]. Выделают пять различных политик сборки. Это даёт нарушителю возможность использовать атаки, основанные на разном времени фрагментации и подмене фрагментов.

В политике, условно называемой First, предпочтение при сборке пакетов из фрагментов отдается фрагментам, полученным раньше, а в политике Last – позже. Политика First реализована в операционных системах семейства Windows, а Last – Cisco iOS. Пример атаки продемонстрирован на рис. 5.

Сначала злоумышленник делит пакет на четыре сегмента с номерами 1, 2, 3, 4 соответственно. Фрагменты 1–3 посылаются первыми, они будут приняты всеми операционными системами. Потом посылаются фрагменты 2', 3' и 4, где фрагменты 2' и 3' содержат новые данные, однако такое же смещение, длину и прочие поля в IP-заголовке, как у оригинальных фрагментов 2 и 3.

В этом случае операционные системы с разными политиками сборки соберут потоки из фрагментов 1, 2, 3 и 4, и из фрагментов 1, 2', 3', 4, т.е. получат совершенно разные данные.

Методика формирования требований к составу качественных характеристик. Проанализировав методы обнаружения атак и ряд современных COA, выяснилось, что способность COA обнаруживать атак в условиях активного уклонения атакующего не учитывается при выборе критериев сравнения.

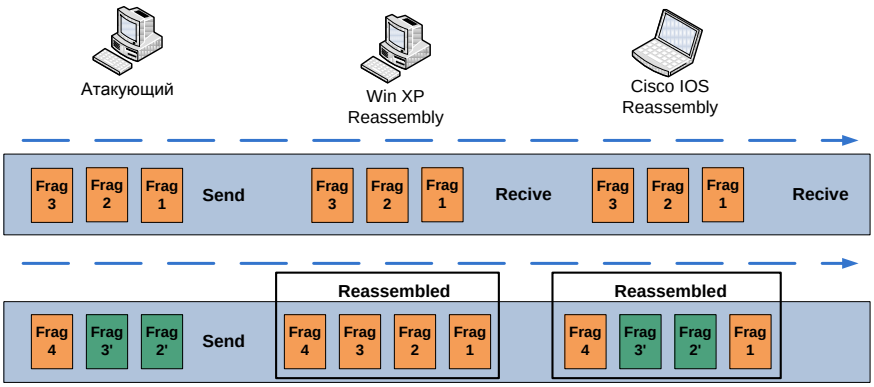

Рис. 5. Политики сборки пакетов

Исходя из вышеописанных методы обхода систем обнаружения атак, можно сформулировать два новых требования к устойчивости работы СОА:

- способность обнаруживать атаки с использованием ресинхронизации;
- способность обнаруживать атаки, связанные со злонамеренной фрагментацией/сегментацией.

Для определения уязвимых мест разработан набор тестов, определяющих, как ведут себя вышеуказанные критические механизмы СОА (табл. 1), [3].

Серия тестов состоит из нескольких групп, различных по назначению.

В результате выполнения тестов работоспособности и правильности конфигурации можно сделать вывод о способности СОА выполнять свои функции.

Таблица 1

Группы тестов для оценки реализации критических функций СОА

Функция СОА	Ожидаемый результат
Определяется, поддерживает ли тестируемая СОА сборку пакетов при наличии злонамеренной фрагментации (out-of-order, дублирующие фрагменты, и т.д.)?	СОА либо производит сборку пакетов, либо в некоторых случаях нет (указывается конкретно).
Определяется способность СОА обрабатывать сложный TCP-трафик в следующих ситуациях: отсутствие ответа от целевого хоста перед тем, как начать обработку данных перехваченных пакетов, нулевое значение номера последовательности или резкое изменение его значения, перекрывающиеся или дублированные сегменты, сегменты в беспорядочном TCP трафике, сборка TCP-сегментов, пришедших не по порядку (out-of-order)?	СОА должна руководствоваться знаниями об известных аномалиях и синхронизироваться с механизмами обработки трафика защищаемой системы, а не следовать RFC.
Определяется, как СОА контролирует TCP-соединение: проверяет ли наличие установленного соединения, перед тем, как начать обрабатывать данные из конкретного соединения, ресинхронизируется при получении SYN-пакета после завершения установки соединения?	СОА не должна проверять наличие соединений и всегда должна ресинхронизироваться.

Окончание табл. 1

Функция СОА	Ожидаемый результат
Определяется, как в СОА осуществляется обработка TCP-данных после формального разрыва соединения: корректно ли ресинхронизируется СОА после легитимного завершения соединения, останавливает ли СОА обработку данных соединения после прихода RST?	СОА не должна прекращать обработку данных, иначе она уязвима для обхода.
Определяется, как в СОА осуществляется обработка аномальных значений полей пакетов: проверяет ли контрольную сумму у принятых IP и TCP пакетов, обрабатывает ли СОА TCP-данные в сегментах без флага ACK?	СОА не должна игнорировать такие пакеты, иначе она уязвима для обхода.
Определяется, поддерживает ли СОА основные функции обнаружения попыток уклонения, такие как, например, контроль передачи данных в SYN-пакетах?	СОА должна обрабатывать такие пакеты.

Состав характеристик для сравнения СОА. С помощью функциональные характеристики оценивают эффективности основной функции СОА – обнаружении атак. При сравнении сетевых СОА, должны оцениваться следующие качественные характеристики СОА:

1. Способность анализировать заголовки – позволяет обнаруживать атаки, связанные со значениями заголовков IP пакетов.
2. Способность собирать фрагментированный трафик – показывает, как в СОА реализованы функции реассемблирования фрагментированного трафика и обнаружения атак, заключенных в нескольких пакетах.
3. Способность обнаруживать атаки, связанные с данными пакетов – позволяет обнаруживать атаки, связанные с данными пакетов.
4. Способность обнаруживать атаки с использованием ресинхронизации – характеризует, как СОА контролирует попытки уклонения с использованием злонамеренных модификаций состояния TCP-соединения.
5. Способность обнаруживать атаки, связанные со злонамеренной фрагментацией/сегментацией – характеризует способность СОА анализировать пакеты, посылаемые в произвольном порядке и с различными временными интервалами между ними, с целью обойти механизм обнаружения.
6. Способность оповещать об инцидентах – характеризует возможности программы оповещать об инцидентах, как локально, так и через электронную почту и SMS.
7. Способность сохранять информацию для анализа – характеризует возможности программы по сохранению информации об инцидентах для дальнейшего анализа.
8. Покрытие базой СОА зарегистрированных уязвимостей (наличие CVE-идентификаторов) – позволяет по формальным признакам оценивать покрытие СОА зарегистрированных уязвимостей; позволяет сравнить различные СОА, использующие разные подходы к обнаружению атак.
9. Архитектура системы принятия решения – показывает, где принимается окончательное решение об обнаружении атаки – на сенсорах или на консоли управления.
10. Цена.

Цель характеристик производительности (количественных характеристик) – определить характеристики работы СОА с пакетами [3].

Выделяют следующие количественные характеристики оценки производительности СОА:

1. Скорость обработки пакетов – позволяет оценить способность СОА перехватывать пакеты не вызывая тревоги;
2. Эффективность фильтрации при решении задачи перехвата и разбора пакета и реагирования на атаку (генерации тревоги) – оценивает общую эффективность системы при решении задачи перехвата, разбора пакета и реагирования на атаку;
3. Производительность сенсора при сборке пакетов – определяет производительность сенсора при сборке пакетов;
4. Влияние работы СОА на производительность системы – позволяет оценить влияния работы СОА на загруженность центрального процессора и памяти, и общую производительность хоста.

Для большей части качественных характеристик установлена зависимость от количественных характеристик [6]. Графически это зависимость представлена на рис. 6.

Рис. 6. Зависимость качественных характеристик от количественных

Заключение. Представленные требования к составу характеристики для оценки СОА позволяют проводить оценку её полезности для пользователя и делать выводы о степени соответствия реальных и заявленных производителем функциональных свойств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Common Intrusion Detection Framework. URL: http://www.gidos.org/ (дата обращения 18.10.2010).
2. *Половко И.Ю. Абрамов Е.С.* Выбор характеристик систем обнаружения атак для выработки заключения о функциональных возможностях СОА // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 88-96.
3. *Ptacek T.H., Newsham T.N.* Insertion, evasion, and denial of service: eluding network intrusion detection. // Technical Report, Secure Networks, January 1998.
4. RFC-792 Протокол ICMP.
5. *Половко И.Ю.* Методы тестирования производительности сетевых СОА // Материалы первой Всероссийской молодёжной конференции по проблемам информационной безопасности «Перспектива 2009». – Таганрог: Изд-во ТТИ ЮФУ, 2009. – С. 192-195.
6. *Половко И.Ю.* Разработка и исследование системы оценки качества СОА. URL: http://www.library.sfedu.ru/referat/D212-208-25/05-13-19/20120323_D212-208-25_05-13-19_PolovkoIY.pdf (дата обращения 21.09.2013).

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

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.