Выводы. Для разработанной многоагентной системы обнаружения атак, применяющей нейронные сети обоих типов, были проведены экспериментальные исследования, подробно описанные в [2]. По результатам экспериментов количество пропусков атак в среднем уменьшилось в 1,1 раза, количество ложных срабатываний в среднем уменьшилось в 3,8 раза. Это позволяет сделать вывод о повышении защищенности информационной системы при применении разработанной многоагентной системы обнаружения атак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Никишова А.В.* Принципы функционирования многоагентной системы обнаружения атак // Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 28-33.
2. *Никишова А.В., Чурилина А.Е.* Обнаружение распределенных атак на информационную систему предприятия // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 135-143.

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Бабенко.

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

Рудиков Роман Федорович – e-mail: rudikovrf@gmail.com; кафедра информационной безопасности; студент.

Калинина Екатерина Александровна – e-mail: kalinina573@gmail.com; кафедра информационной безопасности; студентка.

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

Rudikov Roman Fedorovich – e-mail: rudikovrf@gmail.com; the department of informational security; student.

Kalinina Ekaterina Aleksandrovna – e-mail: kalinina573@gmail.com; the department of informational security; student.

УДК 004.056

И.Ю. Половко, О.Ю. Пескова

АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К СИСТЕМАМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Работа посвящена проблеме оценки качества систем обнаружения вторжений. Проведен сравнительный анализ принятых ФСТЭК требований к системам обнаружения вторжений и перечня функциональных характеристик СОВ. Основной целью данных характеристик является определение функциональных способностей систем обнаружения вторжений (например, обнаружение вторжений в защищаемую сеть, способность сообщать о возникших инцидентах, производить сбор и сохранение информации). Проведенный анализ показал, что принятые требования не позволяют полноценно сравнить функциональные возможности различных систем обнаружения вторжений. Практическое использование принятых требований способствует решению задач классификации СОВ, но не достаточно, чтобы оценить качество реализации функций безопасности в рассматриваемых системами обнаружения вторжений. Для решения вопросов, связанных с оценкой ка-

чества СОВ, а именно – насколько их функциональные возможности позволяют обнаруживать максимум значимых событий, предлагается рассматривать дополнительные функциональные характеристики.

Сетевая безопасность; системы обнаружения вторжений; функциональные требования СОВ.

I.Y. Polovko, O.Y. Peskova

ANALYSIS OF THE FUNCTIONAL REQUIREMENTS FOR INTRUSION DETECTION SYSTEMS

The article work is devoted to the actual problem of assessing of the quality of IDS. The comparative analysis has been done for adopted FSTEC requirements to Intrusion Detection Systems with list of the functional characteristics of IDS. The main goal of these characteristics is to determine the functional abilities of IDS (such as intrusion detections in a protected network, the ability to report any incidents, to collect and store information). The realized analysis showed that the adopted requirements does not allow to compare different intrusion detection systems fully. The practical use of adopted requirements contributes to the solution of practical problems of classification of IDS, but it's not sufficient to assess the quality of implementation of security functions in these intrusion detection systems. To address issues related to the assessment of the quality of IDS - namely, how their functionality can detect a maximum of significant events is proposed to consider additional functional characteristics.

Network security; intrusion detection systems; functional requirements of IDS.

На протяжении долгих лет в Федеральной службе по техническому и экспертному контролю России процедура сертификации для средств обнаружения вторжений была полностью не определена. На сегодняшний день ситуация изменилась.

Для сертификации средств обнаружения вторжений, систем предотвращения утечек данных и подобных элементов в схеме сертификации средств защиты информации ФСТЭК России существовал определенный порядок проведения испытаний. Сертификация таких продуктов до последнего времени проводилась на соответствие «Техническим условиям», что по сути означало полную непредопределенность процесса, поскольку требования к составу функциональных возможностей систем нигде не представлены [1].

Сложившаяся ситуация требовала пересмотра нормативной базы, что послужило причиной принятия ФСТЭК требований к системам обнаружения вторжений (СОВ), доступных на официальном сайте ФСТЭК России.

Общие требования к системам обнаружения вторжений. Система обнаружения вторжений является элементом системы защиты информации в информационных системах, функционирующих на базе нескольких или всех узлов вычислительной сети. Основная задача систем обнаружения вторжений – обеспечение обнаружения и (или) блокирование основных угроз безопасности информации, относящихся к таким вторжениям, как:

- преднамеренный несанкционированный доступ или специальные воздействия на информацию со стороны внешних нарушителей, действующих с использованием информационно-телекоммуникационных сетей;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Системы обнаружения вторжений могут быть пассивными (обнаруживать только факт воздействия на защищаемую систему) или активными (обнаруживать воздействия и выполнять ответные действия по противодействию вторжению).

В состав СОВ входят компоненты регистрации событий (сенсоры или датчики) и компоненты анализа событий и распознавания вторжений (анализаторы), а также при необходимости средства организации взаимодействия.

Состав и стриктура базы решавших правил определяется сочетанием указанных методов обнаружения. В системах обнаружения вторжений реализуются один или совокупность нескольких методов обнаружения вторжений, для примера:

- сигнатурный метод, основанный на базе сигнатур известных вторжений;
- эвристические методы, в основе которых лежат профили функционирования информационной системы или действий пользователей информационной системы.

Помимо вышеперечисленных, в СОВ могут быть реализованы и другие методы обнаружения вторжений [2].

Выделяют следующие типы систем обнаружения вторжений:

1. Системы обнаружения вторжений уровня сети, обеспечивающие сбор информации об информационных потоках, передаваемых в рамках сегмента информационной системы, в котором установлены их датчики.
2. Системы обнаружения вторжений уровня узла (хоста), обеспечивающие сбор информации о событиях, происходящих на узлах информационной системы, на которых установлены их сенсоры (датчики).

Для разделения требования к функциям безопасности системы обнаружения вторжений выделяют шесть классов защиты СОВ. Самый низкий класс – шестой, самый высокий – первый.

Функциональные возможности СОВ определяются набором реализуемых функций безопасности, составом базы решающих правил, используемыми методами обнаружения вторжений, а также имеющимися дополнительными свойствами.

Требования к функциям безопасности СОВ. На основе национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408 [3] установлены требования к функциям безопасности систем обнаружения вторжений, основной состав которых следующий:

1. Разграничение доступа к управлению системой обнаружения вторжений – управление отдельными функциями функций безопасности СОВ, управление данными функций безопасности СОВ, а также распределение ролей управления.
2. Управление работой системы обнаружения вторжений – управление отдельными функциями функций безопасности, интерфейсом, а также системой СОВ в целом.
3. Управление параметрами системы обнаружения вторжений – управление данными функций безопасности СОВ.
4. Управление установкой обновлений базы решающих правил системы обнаружения вторжений – обновление базы решающих правил системы обнаружения вторжений.
5. Анализ данных системы обнаружения вторжений – анализ данных системы обнаружения вторжений.
6. Аудит безопасности системы обнаружения вторжений – генерация данных аудита безопасности, просмотр аудита безопасности.
7. Контроль целостности системы обнаружения вторжений – самотестирование функций безопасности СОВ.
8. Сбор данных о событиях и активности в контролируемой информационной системе – сбор системных данных СОВ, контроль ресурсов, анализ протоколов и избирательный аудит данных СОВ.

9. Реагирование системы обнаружения вторжений – реагирование системы обнаружения вторжений.
10. Маскирование системы обнаружения вторжений – маскирование системы обнаружения вторжений.

Анализ перечисленных функциональных требований показывает, что на их основе не представляется возможным качественно оценить и сравнить функциональные возможности различных систем обнаружения вторжений. Практические использование представленных требований позволяет решить задачу классификации СОВ, но их по-прежнему недостаточно, чтобы оценить качество реализации функций безопасности рассматриваемыми системами обнаружения вторжений.

Перечень функциональных характеристик. Для решения задачи оценки качества СОВ, а именно – насколько функциональные возможности СОВ позволяют обнаруживать максимум значимых событий, предлагается рассматривать дополнительные функциональные характеристики [4].

Функциональные характеристики – это набор характеристик, который служит для оценки деятельности систем обнаружения вторжений в типовой окружающей среде, когда атакующий находится вне сети, в которой расположена СОВ, например, в Internet. Их основная цель – определить функциональные способности систем обнаружения вторжений (например, обнаружение вторжений в защищаемую сеть, способность сообщать о возникших инцидентах, производить сохранение информации).

Основная слабость систем обнаружения вторжений, работающих на сетевом уровне – они принимают решение на основе анализа сетевого трафика, поэтому не могут предсказать, как поведет себя целевая система при получении этого трафика [5]. Помимо этого, СОВ могут быть подвержены атакам отказа в обслуживании (выведение их из строя или исчерпание их ресурсов).

Рассмотрим основные подходы к обходу сетевых СОВ.

Процедура обхода СОВ во многом зависит от мощности ресурсов самой СОВ, чтобы она и целевая система рассматривали разные потоки данных одинаковым образом. Два основных подхода:

1. Если система обнаружения вторжений слабее целевой системы, на которую направлена атака, то при принятии решения, она может рассматривать пакет, который целевая система рассматривать не будет (будет отбрасывать). Атакующий, используя эту возможность, может применить вставку дополнительных пакетов, которые замаскируют атаку для СОВ. Поскольку эти дополнительные (специально сформированные) пакеты будут отброшены целевой системой, атака не будет обнаружена. Например, если СОВ для атаки phf имеет сигнатуру вида GET/ phf, то атакующий может вставить дополнительную информацию, которая замаскирует реальную сигнатуру атаки, например GET/cgi-bin/phf?, или гораздо более длинную строку (помещаемую в пакеты, которые целевая система удалит) вида: GET/cgi-bin/pleasedontdetecthisforme? В этой строке вставлены элементы leasedontdetectl, is, orme, после отбрасывания которых целевая система получит пакет, содержащий phf.

2. Если ресурсы СОВ сильнее чем у целевой системы, то целевая система будет принимать пакеты, которые СОВ не будет рассматривать, что может быть достигнуто использованием метода вставки. Например, для атаки phf атакующий может вставлять элементы данной атаки в пакеты для СОВ с дополнительной информацией. Тогда СОВ отбросит эти пакеты, но они будут рассмотрены целевой системой. Такой подход может позволить замаскировать атаку для системы обнаружения вторжений.

Еще один весьма общим методом обмана СОВ является метод фрагментирования. В нем анализируется различие способностей СОВ и целевой системы в проведении реассемблирования пакетов. Нарушитель может сконструировать последовательность пакетов, которая будет скрывать сигнатуру проводимой атаки, используя знания о силе или слабости системы обнаружения вторжений, по сравнению с целевой системой [6].

При применении метода вставки нарушитель разрушает работу реассемблирования потока данных добавлением пакетов. Кроме того, вставленные пакеты могут перекрывать данные, содержащиеся в исходных фрагментах атаки. При использовании метода обхода нарушитель разрушает реассемблирование потока данных так, чтобы система обнаружения вторжений не рассматривала часть этого потока.

Особенно трудно защититься от атак отказа в обслуживании, направленных против самой СОВ. Это также может быть достигнуто использованием метода вставки большого числа пакетов, чтобы вызвать пропуск системой обнаружения вторжений отдельных пакетов, или применением многочисленной фрагментации [5].

Сетевые СОВ функционируют как «прозрачные» мониторы сетевого трафика, способные обнаруживать аномалии и злоупотребления (сигнатуры). Методы обнаружения аномалий для сетевых СОВ используются редко, из-за потребности в большом периоде времени для построения «нормального» поведения и большого числа ложных срабатываний. Основные методы обхода таких СОВ:

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

Основываясь на проведенных анализах существующих методов и систем обнаружения вторжений, разработан дополнительный перечень функциональных характеристик для СОВ [4]:

1. Способность анализировать заголовки – служит для обнаружения атак, по заголовкам IP пакетов.

2. Способность собирать фрагментированный трафик – функции реассемблирования фрагментированного трафика и обнаружения вторжений, заключенных в нескольких пакетах.

3. Способность обнаруживать атаки, связанные с данными пакетов – позволяет обнаружению атаки в порциях данных пакетов.

4. Способность обнаруживать атаки с использованием ресинхронизации – позволяет провести оценку, как СОВ контролирует попытки уклонения с использованием злонамеренных модификаций состояния TCP-соединения.

5. Способность обнаруживать атаки, связанные со злонамеренной фрагментацией/сегментацией – характеризует способность СОВ 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 – оценивает возможности программы по сохранению информации об инцидентах для дальнейшего анализа.

8. Покрытие базой СОВ зарегистрированных уязвимостей (наличие CVE-идентификаторов) – позволяет по формальным признакам оценивать покрытие СОВ зарегистрированных уязвимостей; позволяет сравнить различные СОВ, использующие разные подходы к обнаружению атак.

9. Архитектура системы принятия решения – дает возможность увидеть, где принимается окончательное решение об обнаружении вторжений – на сенсорах или на консоли управления.

10. Цена.

Особое внимание уделено слабым сторонам протоколов, использование которых позволяет легально обойти механизмы СОВ. При разработчике систем обнаружения вторжений учитываются знания о функционировании протоколов стека TCP/IP. СОВ, основанная на четком следовании RFC, оказывается уязвимой вне зависимости от точности следования, поскольку она имеет свои слабые стороны и уязвимости, что может быть использовано нарушителем для ее обхода или нарушения основных функций.

Выводы. Практические использование представленных требований позволяет решить задачу классификации СОВ, но их по-прежнему недостаточно, чтобы оценить качество реализации функций безопасности рассматриваемыми системами обнаружения вторжений.

В отличие от существующих подходов для оценки СОВ, при разработке дополнительных требований к составу функциональных характеристик для оценки качества СОВ исследовались факторы, которые влияют на эффективность обнаружения вторжений:

- реализация функций, критичных для собственно обнаружения атак;
- реализация функций, критичных для обнаружения попыток уклонения (маскировки) атак;
- реализация функций, критичных для обнаружения попыток обмана (обхода) СОВ
- реализация функций, ответственных за устойчивость перед теми атаками, приоритетной целью которых являются непосредственно СОВ.

Предложенные характеристики могут использоваться для формального сравнения и оценки СОВ и служить основой для выработки заключения о соответствии или несоответствии системы функциональным требованиям.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Барабанов А., Марков А., Цирлов В.* Сертификация систем обнаружения вторжений. Открытые системы. СУБД № 03 2012 г. [Электронный ресурс] URL: http://www.osp.ru/os/2012/03/13015155/ (дата обращения 18.02.2014).
2. Информационное письмо ФСТЭК России об утверждении требований к системам обнаружения вторжений [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/305 (дата обращения 18.02.2014).
3. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Требования доверия к безопасности. – М.: Изд-во стандартов, 2009. – 119 с.
4. *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 23.11.2013).
5. *Ptacek T.H., Newsham T.N.* Insertion, evasion, and denial of service: eluding network intrusion detection // Technical Report, Secure Networks, January 1998.
6. *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.

Статью рекомендовал к рекомендовал к опубликованию к.т.н. М.Н. Казарин.

Половко Иван Юрьевич – 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.

Пескова Ольга Юрьевна – e-mail: poy@tgn.sfedu.ru; кафедра безопасности информационных технологий; к.т.н.; доцент.

Polovko Ivan Yur'evich – 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.

Peskova Olga Yur'evna – e-mail: poy@tgn.sfedu.ru; the department of security of information technologies; cand. of eng. sc.; associate professor.

УДК 004.056.57:004.056.53

Е.С. Абрамов, М.А. Кобилев, Л.С. Крамаров, Д.В. Мордвин

ИСПОЛЬЗОВАНИЕ ГРАФА АТАК ДЛЯ АВТОМАТИЗИРОВАННОГО РАСЧЕТА МЕР ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ

Представлены результаты разработки метода автоматизированного расчета мер противодействия угрозам информационной безопасности сети с использованием графа атак. Описывается алгоритм построения графа атак определенной структуры для оценки уязвимости сети и помощи в более качественном автоматизированном расчете мер противодействия данным уязвимостям. Предлагается алгоритм автоматизированного расчета контрмер, использующий модель сети и взаимодействие с администратором сети (экспертом), обладающим знаниями о специфике сети. Выделяются 11 векторов противодействия уязвимостям. Эксперт осуществляет выбор из предложенных контрмер, для которых предварительно рассчитываются результаты применения и влияние на общую защищённость. Таким образом, применение моделирования позволяет оптимально и с меньшим количеством ошибок распределить правила между межсетевыми экранами, а также скорректировать расположение самих экранов. В результате эксперт может сформировать инструкцию применения контрмер в реальной сети, которая должна стать частью документированной политики информационной безопасности.

Уязвимости; угрозы информационной безопасности; многостадийные атаки; сетевые атаки; контрмеры; межсетвые экраны; системы обнаружения вторжений; CVSS; CVE; IDS; IPS; firewall.

E.S. Abramov, M.A. Kobilev, L.S. Kramorov, D.V. Mordvin

DESIGN OF COUNTERMEASURES FOR SECURITY RISKS OF ENTERPRISE NETWORKS BY USING ATTACK GRAPHS

The article presents the results of the method for automated calculation of countermeasures for network information security threats using attack graph. It describes an algorithm for constructing the attack graph for network vulnerability assessment and for helping in higher quality automated calculation of countermeasures against these vulnerabilities. We propose an algorithm for automated analysis of countermeasures , using a network model and interaction with the network administrator (security executive council), who has knowledge about the specifics of the given network. Allocated 11 vectors counteract vulnerabilities. SEC carries a selection of proposed countermeasures with the pre- calculated results of its application and impact on the overall security. Thus, the use of simulation allows optimal and errorless firewall rules distribution between the firewalls. As a result, the expert can generate instruction of countermeasures in the real network, which should become part of a documented information security policy.

Vulnerabilities; threats to information security; multi-stage attacks; network attacks; countermeasures; intrusion detection systems; CVSS; CVE; IDS; IPS; firewall.