Раздел III. Методы и средства сетевой безопасности

УДК 004.056; 004.8

Е.С. Абрамов, И.Ю. Половко

ВЫБОР ХАРАКТЕРИСТИК СИСТЕМ ОБНАРУЖЕНИЯ АТАК ДЛЯ ВЫРАБОТКИ ЗАКЛЮЧЕНИЯ О ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЯХ

Рассматривается проблема тестирования систем обнаружения сетевых атак. На сегодняшний день не существует стандартизированного подхода к тестированию систем обнаружения сетевых атак, позволяющего выявить все достоинства и недостатки тестируемых систем. Тесты, рекомендуемые производителями, как правило, служат рекламным целям, и не могут помочь оценить функциональные возможности системы. Для решения этой задачи обосновывается набор характеристик для получения качественной оценки и разработан ряд тестов для получения количественных и качественных характеристик тестируемых систем обнаружения сетевых атак.

Система обнаружения атак; оценка эффективности.

E.S. Abramov, I.Y. Polovko

SELECTING OF THE CHARACTERISTICS OF INTRUSION DETECTION SYSTEMS FOR ESTIMATION OF THEIR FUNCTIONAL OPPORTUNITIES

The paper considers the problem of testing systems to detect network attacks. To date, there is no standardized approach to testing systems to detect network attacks, allowing to identify all the advantages and disadvantages of the tested systems. The tests recommended by the manufacturers, tend to serve advertising purposes and cannot help evaluate the functionality of the system. To solve this problem set of specifications for quality assessment is justified and a series of tests for quantitative and qualitative characteristics of the test systems to detect network attacks developed.

Intrusion detection system; performance evaluation.

Тестирование включает в себя рассмотрение количественных и качественных характеристик СОА.

Для проверки количественных характеристик используют:

- функциональное тестирование;
- тестирование производительности.

Для проведения функционального тестирования был разработан набор тестов для оценки деятельности СОА в типовой окружающей среде, когда атакующий находится вне сети, в которой расположена СОА, например, в Internet.

Цель функциональных тестов – определить функциональные возможности СОА (например, способности обнаруживать атаки, сообщать об инцидентах, сохранять информацию). Также эти тесты позволяют установить характеристики СОА при её работе с протоколами TCP/IP и при обнаружении атак. Такие тесты позволяют наиболее полно выявить недостатки тестируемой системы обнаружения атак. Структуризация характеристик СОА с учётом влияния базовых функций на различные характеристики представлена на рис. 1.

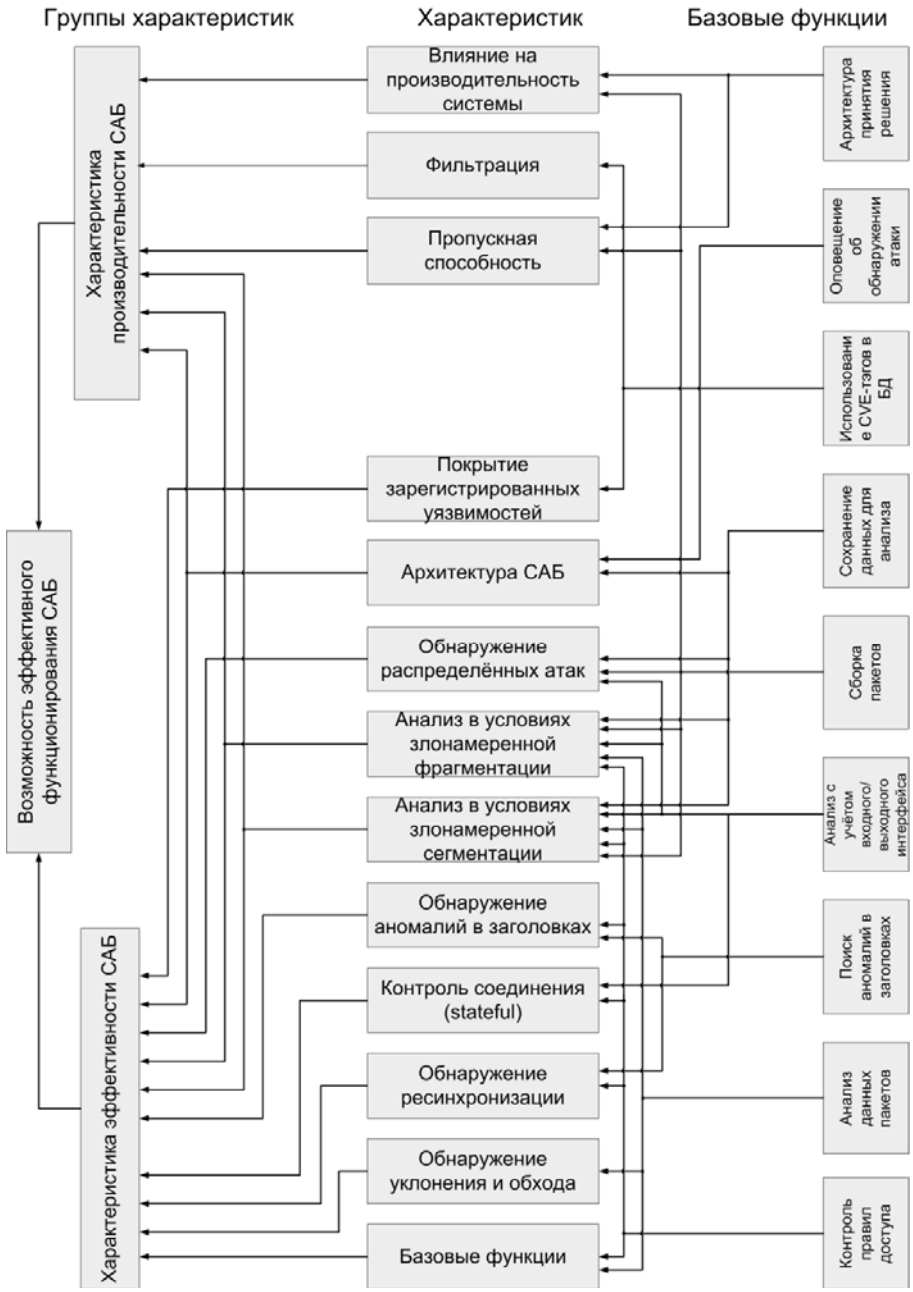

Рис. 1. Структуризация характеристик эффективности СОА с учётом влияния базовых функций на различные критерии

При разработке тестов исследовались функции СОА, 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.

Для определения уязвимых мест разработан набор тестов, определяющих, как ведут себя вышеуказанные критические механизмы COA, с использованием подхода, впервые описанного в [1].

При разработке COA в неё закладываются знания о функционировании протоколов стека TCP/IP. Этот подход обращает внимание на слабые стороны протоколов, использование которых позволяет легально обойти механизмы COA. Таким образом, COA, основанная на следовании RFC, оказывается уязвимой вне зависимости от точности следования [2].

Таблица 1

Группы тестов для оценки реализации критических функций COA

Название теста	Что проверяется?	Ожидаемый результат
baseline	Правильно ли настроена COA?	Подтверждение правильности настройки COA
frag	Поддерживает ли тестируемое COA сборку пакетов при наличии злонамеренной фрагментации (out-of-order, дублирующие фрагменты, и т.д.)?	COA либо производит сборку пакетов, либо в некоторых случаях нет (указываем конкретно)
tcp	Определяется способность COA 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)?	COA должно руководствоваться обнаружением аномалий, а не RFC
tcbc	Определяется, как COA 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?	COA не должно проверять наличие соединений и всегда должно ресинхронизироваться
tcbt	Определяется, как в COA осуществляется обработка TCP-данных после формального разрыва соединения: корректно ли ресинхронизируется COA после легитимного завершения соединения, останавливает ли COA обработку данных соединения после прихода RST?	COA не должна прекращать обработку данных, иначе она уязвима для обхода
insert	Определяется, как в COA осуществляется обработка аномальных значений полей пакетов: проверяет ли контрольную сумму у принятых IP- и TCP-пакетов, обрабатывает ли COA TCP-данные в сегментах без флага ACK?	COA не должна игнорировать такие пакеты, иначе она уязвима для обхода
evade	Определяется, поддерживает ли COA основные функции обнаружения попыток уклонения, такие как, например, контроль передачи данных в SYN-пакетах	COA должна обрабатывать такие пакеты

Результаты функциональных тестов дают ответ об эффективности основных функций СОА – обнаружении атак и фильтрации трафика. Обнаружение атак – способность обнаруживать различные типы атак на основе анализа различных частей пакетов. Таким образом должны оцениваться следующие основные характеристики:

1. Способность анализировать заголовки – позволяет обнаруживать атаки, связанные со значениями заголовков IP-пакетов.
2. Сборка пакетов – возможность СОА собирать фрагментированный трафик и обнаруживать атаки, заключённые в нескольких пакетах.
3. Анализ данных пакета – позволяет СОА обнаруживать атаки, связанные с данными пакетов.
4. Наличие CVE-идентификаторов в базе данных СОА – позволяет по формальным признакам оценивать покрытие (охват) СОА или МЭ зарегистрированных уязвимостей; позволяет сравнить различные СОА, использующие разные подходы к обнаружению атак [4].
5. Способность СОА определять IP Dsync – обнаружение атак, при которых с целью маскировки задаются нестандартные значения номера последовательности и размера.
6. Способность СОА обнаруживать распределённые атаки – выявляются способность СОА, используя метод корреляции, обнаруживать атаки, распределённые во времени (между этапами атаки проходит какое-то время) или в пространстве (атака осуществляется с нескольких хостов с различными IP-адресами).
7. Возможность оповещения – характеризует возможности программы оповещать об инцидентах, как локально, так и через электронную почту и SMS.
8. Возможность сохранения информации для анализа – характеризует возможности программы по сохранению информации об инцидентах для дальнейшего анализа.
9. Наличие распределённой архитектуры – очень важное свойство для СОА, применяющихся в больших сетях. Этот тест определяет архитектуру СОА и показывает способность работы консоли с несколькими сенсорами.
10. Архитектура системы принятия решения – показывает, где принимается окончательное решение об обнаружении атаки – на сенсорах или на консоли управления.
11. Пропускная способность – позволяет оценить способность СОА перехватывать пакеты не вызывая их потерю. Для этого теста был использован только чистый трафик, не содержащий атак.
12. Эффективность фильтрации – предназначен для оценки общей эффективности системы при решении задачи перехвата, разбора пакета и реагирования на атаку. Для тестирования использовалась атака LAND.
13. Влияние на производительность системы – тест для оценки влияния работы СОА на загруженность центрального процессора и памяти и общую производительность хоста [3].

Критерии оценки производительности следующие:

1. Скорость обработки – позволяет оценить способность СОА перехватывать пакеты, не вызывая их потерю.
2. Сборка пакетов – тест для определения производительности сенсора при сборке пакетов.
3. Эффективность фильтрации – тест предназначен для оценки общей эффективности системы при решении задачи перехвата, разбора пакета и реагирования на атаку.
4. Влияние на производительность системы – тест для оценки влияния работы СОА на загруженность центрального процессора и памяти и общую производительность хоста.

Сравнение различных СОА с использованием только их функциональных характеристик и компонентов невозможно, в силу того, что одинаковые задачи, зачастую, решаются при помощи различных компонент. Взаимосвязь характеристик и базовых функций СОА представлена в табл. 2.

Таблица 2

Взаимосвязь критериев и базовых функций СОА

Характеристики	Базовые функции
Способность анализировать заголовки	Проверка механизма СОА по анализу заголовка протокола IP Проверка механизма СОА по анализу заголовка протокола UDP Проверка механизма СОА по анализу заголовка протокола TCP Проверка механизма СОА по анализу заголовка протокола ICMP Фильтрация на сетевом уровне Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов Фильтрация с учетом любых значимых полей сетевых пакетов
Сборка пакетов	Проверка механизма СОА по анализу заголовка протокола IP Проверка возможности анализа поля «Время жизни (TTL)» Проверка возможности анализа поля «Протокол» Фильтрация на сетевом уровне Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов
Анализ данных пакета	Проверка возможности анализа поля «Время жизни (TTL)» Проверка возможности анализа поля «Протокол» Проверка возможности анализа поля «Тип сообщения» Проверка возможности анализа поля «Код сообщения» Проверка возможности анализа длины поля данных Проверка возможности поиска подстроки в поле данных
Способность СОА определять IP Dsync	Проверка возможности анализа длины поля данных Проверка возможности поиска подстроки в поле данных Фильтрация на сетевом уровне Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов Фильтрация с учетом любых значимых полей сетевых пакетов
Способность СОА обнаруживать распределённые атаки	Проверка возможности анализа поля, управляющих фрагментацией пакетов (поля «Идентификатор», «Флаги» и «Смещение») Фильтрация на сетевом уровне Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов Фильтрация с учетом любых значимых полей сетевых пакетов Фильтрация на транспортном уровне запросов на установление виртуальных соединений Фильтрация на прикладном уровне запросов к прикладным сервисам Фильтрация с учетом даты/времени
Возможность оповещения	Локальная сигнализация попыток нарушения правил фильтрации Дистанционная сигнализация попыток нарушения правил фильтрации
Возможность сохранения информации для анализа	Возможность регистрации и учета фильтруемых пакетов. Регистрация и учет запросов на установление виртуальных соединений Регистрация и учет запрашиваемых сервисов прикладного уровня

Окончание табл. 2

Характеристики	Базовые функции
Наличие распределённой архитектуры	Возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети Идентификация и аутентификация администратора МЭ при удалённых запросах на доступ
Архитектура системы принятия решения	Возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети
Пропускная способность	Фильтрация на сетевом уровне. Фильтрация на транспортном уровне. Фильтрация на прикладном уровне запросов Фильтрация с учетом любых значимых полей сетевых пакетов Возможность регистрации и учета фильтруемых пакетов.
Эффективность фильтрации	Фильтрация на сетевом уровне Фильтрация на транспортном уровне Фильтрация на прикладном уровне запросов Фильтрация с учетом любых значимых полей сетевых пакетов Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов Регистрация и учет запросов на установление виртуальных соединений Возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети
Влияние на производительность системы	Фильтрация на прикладном уровне Фильтрация с учетом любых значимых полей сетевых пакетов Идентификация и аутентификация всех субъектов прикладного уровня

Необходимо заметить, что не рассмотрен критерий «Наличие CVE-идентификаторов в базе данных СОА». Этот критерий напрямую не относится к функциональным характеристикам СОА, но позволяет производить формальное сравнение степени покрытия актуальных для защищаемой сети угроз текущей версией базы данных СОА. Поэтому имеет смысл говорить о нём как о синтезированном показателе, косвенно связанным с требованиями к фильтрации. В результате можно увидеть, какие компоненты и функции средств тестирования необходимы для проверки данных характеристик.

При разработке тестов необходимо было решить задачу установления взаимосвязи базовых функций и возможных методов осуществления проверок: примитивные операции – базовые функции – группы базовых функций – характеристики – показатели функционального тестирования). Графически этот процесс представлен на рис. 2.

Каждый тест представляет собой внедрение специальных пакетов в сеть, в которой функционирует тестируемая система обнаружения атак. Результаты тестирования можно отслеживать на консоли управления системой. Тесты универсальны, они воспринимают тестируемую СОА как некий «чёрный ящик». Все тесты используют протокол TCP. В большинстве случаев, в тестах используется взаимодействие между внедрёнными пакетами и третьей стороной – так называемым «целевым» хостом, подвергающимся «атаке». Этот хост является целью назначения всех тестовых пакетов. Наличие такого «целевого» хоста позволяет сымитировать «реальное» TCP-соединение с точки зрения тестируемой СОА. Для этих целей служит эмулятор сетевых сервисов. Кроме того, целевой хост также играет роль проверки эффективности эксперимента.

Рис. 2. Иерархия взаимосвязи базовых функциональных показателей и возможных методов осуществления проверок с критериями

Его реакция на внедрённые пакеты позволяет наблюдать за поведением «реального» TCP-соединения и сравнивать его с информацией о поведении, отображаемой на консоли управления тестируемой СОА.

Перед тем, как проводить комплексные, специальные тесты, проводится серия тестов базовых функций СОА. Цель этих тестов – убедиться, что СОА настроена правильно и функционирует во время проведения тестирования, и что СОА в принципе способна обнаружить атаку.

На целевом хосте для визуализации сетевой активности используется перехватчик пакетов. Контролируя эту активность, можно сказать, должна ли тестируемая СОА вообще обнаружить сымитированную атаку.

Некоторые из предлагаемых проверок связаны с одновременным задействованием нескольких механизмов анализа, однако это не снижает их значимости, поскольку успешное выполнение такой проверки невозможно без корректной работы проверяемого механизма.

Анализ соответствия базовых функций и характеристик СОА (см. табл. 2) позволяет выделить несколько отдельных программных компонент, необходимых для функционального тестирования СОА, и сформулировать требования к составу программно-аппаратного комплекса тестирования:

- генератор сетевых пакетов, позволяющий формировать пакеты для различных типов протоколов, а также различных параметров значений полей, флагов, команд и данных, присущих отдельным типам протоколов;
- имитатор атак – компонент, позволяющий на основе генератора пакетов формировать последовательности пакетов, соответствующие сценариям различных атак;
- перехватчик сетевых пакетов – анализатор сетевого трафика, позволяющий перехватывать максимально возможное число сетевых пакетов из дошедших до сетевого адаптера, осуществлять выборочный перехват пакетов (по настраиваемым фильтрам), осуществлять декодирование заголовков пакета канального, сетевого и транспортного уровней;
- эмулятор сервисов – программный компонент, позволяющий осуществлять сетевое взаимодействие по различным протоколам с возможностью посылать запросы на установление соединения и принимать/передавать данные по настраиваемому порту.

Основные этапы функционального тестирования представлены ниже:

1. Проводится серия базовых тестов СОА с целью определения правильности настройки и функционирования СОА.

2. Узконаправленные тесты представляют собой внедрение специальных пакетов в сеть, в которой функционирует тестируемые средства. Тесты воспринимают тестируемое СОА как «чёрный ящик».
3. Тесты используют протоколы UDP, ICMP и TCP. В большинстве тестов используется TCP-взаимодействие между внедрёнными пакетами и «целевым» хостом, подвергающимся «атаке» и играющим роль проверки эффективности эксперимента.
4. В тестах имитируется «реальное» TCP-соединение с точки зрения тестируемой СОА. Для этих целей служит эмулятор сетевых сервисов.
5. Реакция эмулятора на внедрённые пакеты позволяет наблюдать за поведением «реального» TCP-соединения и сравнивать его с информацией о поведении, отображаемой на консоли управления тестируемого СОА.
6. На целевом хосте для визуализации сетевой активности используется перехватчик пакетов. Контролируя эту активность, можно сказать, должна ли тестируемая СОА вообще обнаружить сымитированную атаку.
7. Анализируя поведение эмулятора и оценивая реакцию СОА на внедрённые пакеты, можно сделать вывод об эффективности реализации функций СОА и установить значения критериев.

Разработанная методика была использованы для тестирования как коммерческой системы обнаружения атак RealSecure for Windows, так и бесплатных – Snort и Bro.

Таблица 3

Результаты тестирования

Характеристика	Snort	RealSecure	Bro
Функциональное тестирование (оценка от 0 до 10)			
Способность анализировать заголовки	10	9	6
Сборка пакетов	8	5	4
Анализ данных пакета	9	9	9
Способность СОА определять IP Dsync	7	2	0
Способность СОА обнаруживать распределённые атаки	7	8	0
Возможность оповещения	7	8	7
Возможность сохранения информации для анализа	10	10	8
Тестирование производительности			
Пропускная способность	~80 Мбит/с	~80 Мбит/с	65 Мбит/с
Эффективность фильтрации (80 Мбит/с), пакетов потеряно	2 %	2 %	15 %
Влияние на производительность системы	14,7 %	42 %	16 %

Результаты показали уязвимость RealSecure при наличии злонамеренной фрагментации, что можно отнести к использованию механизма обработки фрагментированного трафика, схожего с тем, что использует Windows, и относительной «старостью» данной СОА. Кроме того, RealSecure и Bro показали слабую эффективность при сборке TCP-сегментов, пришедших не по порядку в условиях множественных перекрывающихся и дублированных сегментов. Это обусловлено слишком точным следованием RFC, что снижает эффективность обнаружения аномалий. Все исследованные системы оказались уязвимы при обработке ресинхронизации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. Thomas H. Ptacek, Timothy N. Newsham [Электронный ресурс] / Режим доступа: http://insecure.org/stf/secnet_ids/secnet_ids.html, свободный. – Загл. с экрана.
2. Network Based Intrusion Detection. A review of technologies. [Электронный ресурс] / Режим доступа: http://linkinghub.elsevier.com/retrieve/pii/S01674048998 0131X, свободный. – Загл. с экрана.
3. Benchmarking network IDS. [Электронный ресурс] / Режим доступа: http://archives.neohapsis.com/ archives/sf/ids/2000-q4/0244.html, свободный. – Загл. с экрана.
4. Common Vulnerabilities and Exposures [Электронный ресурс] / Режим доступа: http://Cve.mitre.org, свободный. – Загл. с экрана.

Статью рекомендовал к опубликованию к.т.н., доцент О.Б. Спиридонов.

Абрамов Евгений Сергеевич
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: abramoves@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 88634371905.
Кафедра безопасности информационных технологий; к.т.н.; доцент.

Половко Иван Юрьевич
E-mail: ivan.polovko@mail.ru.
Кафедра безопасности информационных технологий; аспирант.

Abramov Evgeny Sergeevich
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: abramoves@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: +78634371905.
The Department of Security in Data Processing Technologies; Cand. of Eng. Sc.; Associate Professor.

Polovko Ivan Yur’evich
E-mail: ivan.polovko@mail.ru.
The Department of Security in Data Processing Technologies; Postgraduate Student.

УДК 519.254, 004.056

В.А. Нестеренко, А.А. Таран

РЕДУКЦИЯ РАЗМЕРНОСТИ ПРОСТРАНСТВА СОСТОЯНИЙ В ЗАДАЧАХ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Статья посвящена рассмотрению возможности уменьшения числа характеристик используемых при анализе состояния системы. Задача снижения числа характеристик очень важна при разработке и создании систем обнаружения вторжений: С увеличением числа характеристик улучшается качество систем обнаружения вторжений, с одной стороны, и уменьшается призводительность и быстродействие, с другой стороны. Рассмотрены два метода: метод главных компонент (principal component analysis – PCA) и линейный дискриминантный анализ Фишера (Fisher's linear discriminant analysis – LDA). Проводится оценка эффективности этих методов и примеры их практического использования при анализе сетевого трафика.

Метод главных компонент; линейный дискриминантный анализ; алгоритм Фишера; снижение размерности данных; обнаружение вторжений; анализ сетевого трафика.