Министерство образования Республики Беларусь

ПОЛОЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра вычислительных систем и сетей

**Методические указания по выполнению лабораторной работы № 2 по курсу «Защита информационных ресурсов компьютерных систем и сетей»**

Обнаружение аномальной активности сети

Доцент,

кандидат технических наук,

Раханов Константин Яковлевич

**Полоцк, 2015**

**Содержание**

[Перечень условных сокращений 3](#_Toc399971678)

[Теоретические сведения 4](#_Toc399971679)

[Обнаружение в реальном времени и отложенный анализ 7](#_Toc399971680)

[Локальные и сетевые системы обнаружения атак 8](#_Toc399971681)

[Распределенные системы обнаружения атак 10](#_Toc399971682)

[Типовая архитектура СОА 11](#_Toc399971683)

[Цель работы 12](#_Toc399971684)

[Требования, предъявляемые к лабораторной работе 13](#_Toc399971685)

[Ход выполнения работы 13](#_Toc399971686)

[Содержание отчета 13](#_Toc399971687)

**Перечень условных сокращений**

СОА – Система обнаружения атак

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

ИС – Информационная система

МЭ – Межсетевой экран

АС – Автоматизированная система

**Теоретические сведения**

Мониторинг и анализ сетевого трафика являются неотъемлемой частью процесса управления компьютерной сетью и используются для диагностики, тестирования и поиска неисправностей, для оптимизации структуры информационных потоков, а также выявления и решения проблем в обеспечении безопасности.

**Система обнаружения атак** (СОА) — это программный или программно-аппаратный комплекс, предназначенный для выявления и по возможности предупреждения действий, угрожающих безопасности информационной системы.

Первые прототипы СОА появились в начале 1980-х годов и были ориентированы в первую очередь на защиту автономных ЭВМ, не объединенных в сеть. Обнаружение атак производилось путем анализа журналов регистрации событий постфактум. Современные системы в основном ориентированы на защиту от угроз, направленных из сети, поэтому их архитектура существенным образом поменялась. Вместе с тем основные подходы к обнаружению атак остались прежними.

Сигнатурный анализ основан на предположении, что сценарий атаки известен и попытка ее реализации может быть обнаружена в журналах регистрации событий или путем анализа сетевого трафика. В идеале администратор информационной системы должен устранить все известные ему уязвимости. На практике, однако, данное требование может оказаться невыполнимым, так как в результате может существенным образом пострадать функциональность ИС. Не исключено также, что людские и материальные затраты, необходимые для устранения этих уязвимостей, могут превысить стоимость информации, обрабатываемой системой. Системы обнаружения атак, использующие методы сигнатурного анализа, предназначены для решения обозначенной проблемы, так как в большинстве случаев позволяют не только обнаружить, но и предотвратить реализацию атаки на начальной стадии ее выполнения.

Процесс обнаружения атак в данных системах сводится к поиску заранее известной последовательности событий или строки символов в упорядоченном во времени потоке информации. Механизм поиска определяется способом описания атаки.

Наиболее простым является описание атаки при помощи набора правил (условий). Применительно к анализу сетевых пакетов эти правила могут включать определенные значения отдельных полей заголовка пакета (IP-адрес и порт источника или получателя, установленные флаги, размер пакета и т. д.).

При анализе журналов регистрации событий правила могут ограничивать время регистрации пользователя в системе, количество попыток неправильного ввода пароля в течение короткого промежутка времени, а также наличие изменений в критических файлах системы. Таким образом, описание атаки отражает, во-первых, характер передаваемой информации и, во-вторых, совокупность реакций системы на реализацию атаки.

Если описать текущее состояние информационной системы совокупностью пар атрибут-значение, а события представить как действия, связанные с изменением этих атрибутов, то для описания атаки может использоваться теория конечных автоматов. В этом случае реализации каждой атаки соответствует последовательность переходов из «исходного» состояния системы в ее «конечное» состояние, характеризующее реализацию данной атаки. Условия и направление перехода определяются набором правил, как было описано выше. Такой подход к описанию сценария атаки является более точным, чем описание при помощи набора правил, так как позволяет учитывать динамику развития атаки и выявлять попытки реализации атак, скрытых в интенсивном потоке событий, сгенерированных злоумышленником для прикрытия своих истинных намерений.

Применение методов сигнатурного анализа требует от разработчика СОА выбора или создания специального языка, позволяющего описывать регистрируемые системой события, а также устанавливать соответствия между ними. Универсальность и полнота этого языка являются определяющими факторами эффективной работы системы обнаружения, так как в конечном счете на этом языке будут сформулированы правила, по которым выявляется атака.

Реагирование на попытку реализации атаки может включать как простое извещение администратора информационной системы, так и более активные меры: разрыв установленного соединения, отключение уязвимой службы, перепрограммирование межсетевого экрана на отклонение пакетов, полученных от выявленного системой злоумышленника, а также другие меры, препятствующие «успешному» завершению атаки.

Все СОА, использующие метод обнаружения атак по сигнатуре, имеют в своем составе базу данных известных атак (их сигнатур). Очевидно, что к принципиальным недостаткам рассматриваемого класса СОА относится невозможность обнаружения атак, сигнатуры которых отсутствуют в базе данных. Поэтому, чтобы обеспечить эффективную работу системы обнаружения, эта база должна регулярно обновляться. Обычно возможность обновления, в том числе автоматического, предусмотрена разработчиками системы. Преимуществами систем, использующих сигнатурный анализ, являются низкая вероятность «ложной тревоги» (ошибочного обнаружения атаки при ее фактическом отсутствии), а также относительная простота настройки.

Подход к обнаружению атак, основанный на попытке обнаружения аномального поведения системы, также был впервые предложен в 1980-х годах. Основной предпосылкой применения указанного подхода является то, что в процессе «штатного» функционирования информационная система находится в некотором равновесном состоянии. Попытка реализации атаки ведет к выходу системы из этого состояния, причем факт выхода может быть зафиксирован. При создании СОА, работающих по принципу обнаружения аномалий, должны быть решены три задачи. Во-первых, необходимо разработать способ описания состояния информационной системы. Это нетривиальная задача, так как должна быть учтена как статическая, так и динамическая составляющие. Например, должны быть описаны типичные для системы потоки данных, передаваемых по сети. Во-вторых, необходимо разработать алгоритмы, при помощи которых будет автоматически (или с вмешательством администратора) составляться описание реальной работающей системы — ее «профиль». Это нужно для того, чтобы «научить» СОА различать штатный режим работы информационной системы. В-третьих, необходимо выбрать математические методы, которые будут использоваться для обнаружения аномалий в процессе функционирования системы. Другими словами, должны быть определены механизмы принятия решения о попытке атаки защищаемой системы. Очевидно, что используемые механизмы принятия решения в первую очередь зависят от того, как была описана система.

Рассмотрим простой пример. Пусть одним из параметров информационной системы является количество отклоненных входящих TCP-соединений, а точнее — среднее значение и дисперсия указанного параметра. В случае штатной работы системы количество отклоняемых соединений должно быть незначительным. Если злоумышленник начнет исследовать уязвимость системы при помощи сканирования портов, то есть попытается реализовать атаку «сканирование портов», количество отклоненных TCP-соединений резко возрастет. Такой скачок может быть обнаружен различными способами. Во-первых, может быть применен статистический критерий равенства средних значений двух случайных величин. Для его использования, правда, необходимо сделать два достаточно неоднозначных предположения: о нормальности распределений случайных величин и о равенстве их дисперсий. Во-вторых, что представляется более уместным, могут быть применены математические методы, известные под общим названием «методов обнаружения разладки». Эти методы специально разрабатывались для решения подобного класса задач, первоначально связанных с контролем систем слежения и управления. В-третьих, могут применяться математические методы распознавания образов. Известны также разработки, использующие нейросетевые методы анализа, однако о практическом внедрении этих методов в коммерческих программных продуктах до сих пор не сообщается.

Основным преимуществом использования подхода, основанного на обнаружении аномального поведения системы, является теоретическая возможность обнаружения новых, не описанных ранее, атак. Данная возможность основана на предположении, что атака по определению представляет собой набор действий, нехарактерных для штатного режима работы системы. Насколько эффективно будут выявляться новые атаки, определяется опять же способом описания состояния системы и количеством анализируемых параметров.

Большинство математических методов обнаружения, используемых в рассматриваемом классе СОА, не являются детерминированными. Это означает, что все решения принимаются на основе статистического анализа и, следовательно, могут содержать ошибки. Возможны два класса ошибок: «пропуск атаки» и «ложная тревога».

Вероятность пропуска определяется характером атаки и степенью адекватности описания текущего состояния системы. «Ложная тревога» может иметь место в том случае, если в информационной системе наблюдается нетипичная активность, являющаяся следствием действий законных пользователей (или процессов). Например, если на всех компьютерах локальной сети, имеющей подключение к Интернет, будет установлена антивирусная программа, запрограммированная на обновление антивирусных баз в одно и то же время каждые два дня, то одновременная попытка всех компьютеров подключиться к одному серверу Интернет будет интерпретироваться СОА как вирусная атака. Поэтому именно высокую вероятность «ложной тревоги» обычно называют главным недостатком систем обнаружения атак, основанных на обнаружении аномальной активности. Еще одним недостатком принято считать сложность настройки («обучения») системы, так как этот процесс требует от администратора глубоких знаний базовых принципов взаимодействия элементов информационной системы.

В связи с этим полноценных коммерческих продуктов, использующих принципы обнаружения аномальной активности, на рынке практически нет, хотя разработки этих систем непрерывно ведутся ввиду их перспективности.

**Обнаружение в реальном времени и отложенный анализ**

По типу обрабатываемых данных системы обнаружения атак подразделяются на «системы реального времени» и «системы отложенной обработки». Системы отложенной обработки анализируют содержимое журналов регистрации событий или массив предварительно записанного трафика, а системы реального времени — входящий поток событий от программных датчиков. Очевидно, что адекватное реагирование на попытку реализации атаки, включая ее предотвращение, возможно только при использовании систем реального времени. В то же время это не означает, что СОА реального времени «лучше», чем системы отложенной обработки. Так, СОА реального времени, не имеющая функций по предотвращению атак, заведомо менее эффективна, чем аналогичная система с отложенной обработкой, поскольку в системе реального времени одним из основных критериев эффективности является простота используемых алгоритмов, а не их оптимальность с позиций надежности обнаружения атак. Поэтому выбор того или иного типа СОА должен делаться исходя из анализа задач, которые ставятся перед системой обнаружения.

Апостериорный анализ может использоваться со следующей целью:

* расследование информационных преступлений и инцидентов;
* выявление атак, не являющихся информационным преступлением (сбор информации об инфраструктуре сети, сканирование портов и пр.);
* сбор информации об уязвимостях информационной системы с целью их устранения;
* анализ активности отдельных пользователей;
* минимизация

Основным фактором, определяющим защищенность автоматизированной системы (АС) от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

**Локальные и сетевые системы обнаружения атак**

СОА, использующие информацию, получаемую от персонального компьютера, на который они установлены, обычно называют локальными (*host-based*). В противоположность им системы обнаружения, ориентированные на анализ всего доступного сетевого трафика, называют сетевыми (*network-based*).

Рассмотрим, какая информация может использоваться локальными СОА для выявления попыток атаки.

− Отслеживание попыток входящих и исходящих TCP- и UDP-соединений. В результате могут обнаруживаться и пресекаться попытки несанкционированных подключений к отдельным портам, а также попытки сканирования портов.

− Анализ входящего и исходящего сетевого трафика на предмет наличия «подозрительных» пакетов. «Досмотру» могут подлежать как поля заголовков пакетов, так и их содержимое.

− Отслеживание попыток регистрации на локальной ЭВМ. В случае интерактивной регистрации может накладываться ограничение на время регистрации, а в случае регистрации по сети можно ограничить перечень сетевых адресов, с которых разрешается вход в систему. Отдельное внимание уделяется множественным неудачным попыткам регистрации, которые могут иметь место в случае атаки «подбор пароля методом перебора».

− Отслеживание активности пользователей, наделенных повышенными полномочиями в системе (суперпользователь root в UNIX-системах, пользователи группы Администраторы в ОС Windows). Так как в широком классе случаев атака направлена на получение полномочий суперпользователя, могут отслеживаться попытки регистрации этого пользователя в системе в неразрешенное время, попытки сетевой регистрации суперпользователя и т. д.

− Проверка целостности отдельных файлов или ключей реестра (для Windows-систем). Несанкционированные действия взломщика могут заключаться в попытках внесения изменений в базу данных пользователей или в модификации отдельных настроек системы. Контроль целостности критичных областей данных позволит СОА обнаружить попытку реализации атаки. Сетевые СОА собирают и анализируют все доступные им сетевые пакеты на предмет наличия «подозрительного» содержимого или несанкционированных потоков информации от одного узла сети к другому. В связи с этим точка подключения СОА должна обеспечивать максимальный охват трафика, циркулирующего в сегменте сети.

Обычно такие системы подключаются к специальному порту коммутатора либо устанавливаются непосредственно на маршрутизаторе сети. СОА данного класса гораздо эффективнее, чем локальные, способны обнаруживать факт сканирования портов, а также выявлять попытки атак на «отказ в обслуживании». Кроме того, если система обнаружения установлена на шлюзе, обеспечивающем доступ из локальной сети в Интернет, то путем фильтрации нежелательных пакетов может обеспечиваться защита этой локальной сети от внешних атак. Получается, что СОА выполняет в этом случае функции межсетевого экрана (либо управляет им). Таким образом, сетевые системы обнаружения атак находят свое применение в информационных системах, где установка специализированного программного обеспечения на компьютеры пользователей затруднительна, и там, где требуется изолировать сетевой сегмент от внешней угрозы.

Необходимо отметить, что анализ интенсивного потока данных требует существенных вычислительных затрат, поэтому аппаратные требования к узлу, на котором устанавливается такая СОА, могут быть очень высокими. Наиболее критичной эта проблема становится при попытке защиты сети, содержащей несколько сотен компьютеров и имеющей выход в Интернет. К этому классу относятся большинство сетей крупных предприятий.

**Распределенные системы обнаружения атак**

Отдельным классом систем обнаружения атак являются распределенные системы. Их основным отличием является перераспределение функций сбора данных между несколькими «агентами» — программными датчиками, установленными на узлах информационной системы. Агенты могут собирать информацию непосредственно с компьютера, на который они установлены, или анализировать данные, передаваемые по сети. Наиболее принципиальным моментом при внедрении распределенных СОА является организация информационного обмена между отдельными агентами системы. Конечной целью этого обмена является принятие решения о факте атаки.

Преимуществом использования распределенных систем является возможность собирать и анализировать значительно больший объем информации, что позволяет обнаруживать широкий спектр атак. В этом отношении наиболее эффективным является решение, объединяющее методологию локальных и сетевых СОА в единое целое. С другой стороны, распределенные системы обладают рядом недостатков, наиболее существенным из которых является меньшая защищенность их компонентов. Во-первых, сбор данных с нескольких узлов создает дополнительную нагрузку на сеть, которая, в случае полномасштабной атаки, может превысить ее пропускную способность. Во-вторых, обмен информацией по сети подразумевает наличие открытых портов, потенциально доступных для атаки на отказ в обслуживании (переполнение очереди входящих TCP-соединений). В-третьих, на узлах информационной системы возможно внедрение вредоносного программного обеспечения, которое будет блокировать работу агента или пытаться подделывать информацию, им передаваемую.

Отдельной задачей, возникающей при проектировании распределенных СОА, является выбор идеологии процедуры принятия решения. Возможны несколько вариантов процедуры, отличающиеся степенью централизации. Наиболее простым является вариант процедуры с предельной степенью централизации, когда агенты занимаются лишь сбором данных и передачей их центральному узлу СОА — модулю принятия решения. Этот модуль анализирует поступающую информацию и выносит решение о факте атаки. Данный вариант характеризуется большим объемом передаваемых по сети данных, что повышает вероятность обнаружения факта работы СОА злоумышленником и делает систему уязвимой к атакам на отказ в обслуживании. Наиболее очевидным решением по использованию такого типа СОА является их установка в рамках подсетей небольшого размера, что позволит обойти проблему перегрузки сети пакетами, сгенерированными системой. Увеличение масштабов сети требует многоступенчатого подхода к принятию решения. Он заключается в том, что выделяются промежуточные модули принятия решения, которые собирают данные только с ограниченного числа «своих» агентов и передают на верхний уровень гораздо меньший объем информации, дополненный промежуточным решением. При любом варианте реализации процедуры принятия решения очевидно, что первоочередной становится задача обеспечения защищенности самой СОА.

В настоящее время СОА начинают все шире внедряться в практику обеспечения безопасности корпоративных сетей. Однако существует ряд проблем, с которыми неизбежно сталкиваются организации, развертывающие у себя систему выявления атак. Эти проблемы существенно затрудняют, а порой и останавливают процесс внедрения IDS. Вот некоторые из них:

* высокая стоимость коммерческих СОА;
* невысокая эффективность современных СОА, характеризующаяся большим числом ложных срабатываний и несрабатываний (false positives and false negatives);
* требовательность к ресурсам и порой неудовлетворительная производительность СОА уже на 100 Мбит/с сетях;
* недооценка рисков, связанных с осуществлением сетевых атак;
* отсутствие в организации методики анализа и управления рисками, позволяющей адекватно оценивать величину риска и обосновывать стоимость реализации контрмер для руководства;
* высокая квалификация экспертов по выявлению атак, требующаяся для внедрения и развертывания СОА.

**Типовая архитектура СОА**

Типовая архитектура системы выявления атак, как правило, включает в себя следующие компоненты:

1. Сенсор (средство сбора информации);
2. Анализатор (средство анализа информации);
3. Средства реагирования;
4. Средства управления.

Эти компоненты могут функционировать и на одном компьютере и даже в рамках одного приложения, однако чаще всего они территориально и функционально распределены. Такие компоненты СОА, как анализаторы и средства управления, опасно размещать за МЭ во внешней сети, т. к. если они будут скомпрометированы, то злоумышленник может получить доступ к информации о структуре внутренней защищаемой сети на основе анализа базы правил, используемой СОА.

Типовая архитектура системы выявления атак изображена на рисунке. Сетевые сенсоры осуществляют перехват сетевого трафика, хостовые сенсоры используют в качестве источников информации журналы регистрации событий ОС, СУБД и приложений. Информация о событиях также может быть получена хостовым сенсором непосредственно от ядра ОС, МЭ или приложения. Анализатор, размещаемый на сервере безопасности, осуществляет централизованный сбор и анализ информации, полученной от сенсоров.

**Рисунок. Типовая архитектура СОА**

Средства реагирования могут размещаться на станциях мониторинга сети, МЭ, серверах и рабочих станциях ЛВС. Типичный набор действий по реагированию на атаки включает в себя оповещение администратора безопасности (средствами электронной почты, вывода сообщения на консоль или отправки на пэйджер), блокирование сетевых сессий и пользовательских регистрационных записей с целью немедленного прекращения атак, а также протоколирование действий атакующей стороны.

Средства управления предназначены для администрирования всех компонентов системы выявления атак, разработки алгоритмов выявления и реагирования на нарушения безопасности (политик безопасности), а также для просмотра информации о нарушениях и генерации отчетов.

**Цель работы**

Разработать систему обнаружения аномальной активности в сети, в состав которой входит сетевой сенсор и анализатор активности.

**Требования, предъявляемые к лабораторной работе**

Язык программирования: определяется студентом.

Алгоритм обнаружения аномальной активности в сети: определяется студентом.

Обязательные компоненты, которые должны быть реализованы:

* сетевой сенсор для мониторинга трафика всей локальной сети. Сетевой сенсор должен переводить сетевой адаптер в режим «беспорядочного» приема кадров;
* анализатор событий для обнаруживает аномальной активности;
* модуль реагирования для уведомления о наличии аномальной активности либо блокировки ресурсов;
* модуль логирования.

**Ход выполнения работы**

1. Изучить теоретические сведения, ознакомиться со структурой систем обнаружения атак, принципами их работы.
2. Выбрать технологию разработки, разработать структуру приложения
3. Реализовать приложение для обнаружения аномальной активности в локальной сети
4. Написать отчет о проделанной работе.
5. Защитить отчет.
6. Предоставить отчет и исходные коды приложения в архиве (формат архива: «ZIRKSiS\_Lab\_2\_IT-1\_Фамилия\_на\_транслите.zip»).

**Содержание отчета**

1. Титульный лист, содержащий пункты «Разработал», «Проверил».
2. Описания реализации приложения с листингом основных функций, скриншотами, демонстрирующими работу приложения.
3. Вывод о функционировании полученного приложения, содержащий СОБСТВЕННОЕ заключение о результатах работы приложения.