# Обзор зарубежных и отечественных систем обнаружения компьютерных атак

## Review of foreign and domestic computer attacks detection systems

**Бабошин**
Владимир Александрович
(boboberst@mail.ru)
кандидат технических наук, доцент.
ОАО «Научно-исследовательский институт «Рубин»,
начальник отдела.
г. Санкт-Петербург

**Голубев**
Владимир Ефимович
(inforubin@rubin-spb.ru)
кандидат военных наук, доцент.
ОАО «Научно-исследовательский институт «Рубин»,
главный специалист.
г. Санкт-Петербург

**Васильев**
Виктор Афанасьевич
(viktor-vasilev-1946@mail.ru)
кандидат технических наук, доцент.
ФГКВОУ ВПО »Военно-космическая академия
имени А. Ф. Можайского» МО РФ,
доцент кафедры технологий и средств технического
обеспечения и эксплуатации АСУ (войсками).
г. Санкт-Петербург

Ключевые слова: информационная безопасность – information security; система обнаружения атак – atack detection system; система обнаружения вторжений – intrusion detection system; детектор атак – attack detector.

В статье рассматривается проблема информационной безопасности инфокоммуникационных систем, связанная с необходимостью защиты от компьютерных атак, а также классификация и некоторые особенности построения систем обнаружения компьютерных атак (Intrusion Detection Systems-IDS) как зарубежной, так и отечественной разработки. Рассмотрены особенности построения распределенной системы обнаружения атак, в том числе и на основе динамического анализа сетевого трафика, назначение и основные функции детектора атак.

Information security of infocommunication systems problem according to necessity of computer attack protection, classification and some issues of intrusion detection system (IDS) building as domestic and foreign development are considered in the article. Issues of distributed attack detection systems including that are based on network traffic dynamic analysis, purpose and attack detector common function are considered.

### Введение

Оценка современного состояния существующих и вновь создаваемых перспективных инфокоммуникационных систем и сетей специального назначения, к которым относятся и системы и сети ВКО, свидетельствует о наличии научно-технической проблемы создания единой государственной системы обнаружения, предупреждения и ликвидации компьютерных атак. На рынке продуктов средств информационной безопасности имеется довольно ограниченный перечень отечественных систем обнаружения атак (вторжений), сертифицированных органами Федеральной службы безопасности (ФСБ) России или органами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России. Вследствие остроты обозначенной проблемы задача построения единой государственной системы обнаружения, предупреждения и ликвидации компьютерных атак является одной из приоритетных в Российской Федерации, направленной на исполнение Указа Президента Российской Федерации «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15.01.2013 г. [1].

С целью обеспечения информационной безопасности Гостехкомиссия России разработала основополагающие руководящие документы по обеспечению защиты информации [2, 3], которыми должны руко-

водствоваться органы государственной власти, организации, предприятия, оборонные ведомства, силовые структуры, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом.

Проблема обеспечения информационной безопасности должна решатся, в том числе, путем разработки и применения высокоэффективных систем обнаружения, предупреждения и ликвидации компьютерных атак (вторжений) на основе знания современного состояния зарубежных систем компьютерных атак и информационной безопасности в существующих отечественных инфокоммуникационных системах и сетях специального назначения.

## Зарубежные системы обнаружения компьютерных атак

Зарубежные системы обнаружения компьютерных атак (IDS – Intrusion Detection Systems) являются в настоящее время важнейшим элементом систем информационной безопасности специальных сетей.

В ряде зарубежных документов предлагается ранжировать различные типы атак в соответствии с возрастанием их возможной опасности [4, 5]:

– угадывание паролей;
– репликационный код;
– взлом паролей;
– использование известных уязвимых мест;
– отключение/обход систем аудита;
– воровство данных;
– специальные входы в программу, возникающие из-за ошибок при ее написании или оставленные программистами для отладки (back doors);
– использование систем контроля содержимого (снифферов и sweepers);
– использование программ диагностики сети для получения необходимых данных;
– использование автоматизированных сканеров уязвимостей;
– подмена данных в IP-пакетах;
– атаки типа «отказ в обслуживании» (DoS);
– атаки на Web-серверы (CGI-скрипты);
– технологии скрытого сканирования;
– распределенные средства атаки.

Известны и применяются на практике различные способы классификации IDS.

Например, по способу реагирования различают пассивные и активные IDS. Пассивные IDS фиксируют факт атаки, записывают данные в файл журнала и выдают предупреждения. Активные IDS пытаются противодействовать атаке, например за счет реконфигурации межсетевого экрана или путем генерации списков доступа маршрутизатора.

По способу выявления атаки различают системы signature-based и anomaly-based. Первый тип основан на сравнении информации с предустановленной базой сигнатур атак. В свою очередь, можно классифицировать атаки по типу (например, Ping-of-Death, Smurf). Однако системы данного типа не могут отлавливать новые, неизвестные виды атак. Второй тип основан на контроле частости событий или обнаружении статистических аномалий. Такая система ориентирована на выявление новых типов атак. Недостатком системы является необходимость постоянного обучения.

Наиболее распространена классификация по способу сбора информации об атаке (network-based, host-based, application-based).

Системы первого типа (network-based) работают по типу сниффера, «прослушивая» трафик в сети и определяя возможные действия злоумышленников. Поиск атаки идет по принципу «от хоста до хоста». Работа таких систем была затруднена в сетях, в которых использовались коммутация, шифрование и высокоскоростные протоколы (более 100 Мбит/с). Появились решения компаний NetOptics (http://www.netoptics.com) и Finisar (http://www.finisar.com) для работы в коммутируемой среде, в частности, технологии SPAN-портов (Switched Port Analyzer) и Network Tap (Test Access Port). Изделие Network Tap (в виде отдельного устройства или встроенного в коммутатор блока) позволяет осуществлять мониторинг всего трафика на коммутаторе. Компании Cisco и ISS добились определенных успехов в реализации таких систем для высокоскоростных сетей.

Системы второго типа (host-based) предназначены для мониторинга, детектирования и реагирования на действия злоумышленников на определенном хосте. Средства системы располагаются на защищаемом хосте, проверяют и выявляют направленные против него действия.

Третий тип IDS (application-based) основан на поиске проблем в определенном приложении.

Существуют также гибридные IDS, представляющие собой комбинацию различных типов систем.

Общая схема функционирования IDS приведена на рис. 1.

В последнее время появилось много публикаций о системах, называемых distributed IDS (dIDS). Система dIDS состоит из множества IDS, которые расположены в различных участках сети и связаны между собой и с центральным управляющим сервером. Такая система усиливает защищенность корпоративной подсети благодаря централизации информации об атаке от различных IDS. Система dIDS содержит центральный анализирующий сервер, агентов сети, сервер сбора информации об атаке.

Центральный анализирующий сервер обычно содержит Web-сервер и базу данных, что позволяет сохранять информацию об атаках и манипулировать данными с помощью удобного Web-интерфейса.

Агент сети – один из наиболее важных компонентов dIDS. Агент представляет собой программу, цель которой сообщать об атаке на центральный анализирующий сервер.

Сервер сбора информации об атаке – часть системы dIDS, логически базирующаяся на центральном анализирующем сервере. Сервер определяет параметры, по которым группируется информация, полученная от агентов сети. Группирование может осуществляться по следующим параметрам:

– IP-адресу атакующего;
– порту получателя;
– номеру агента;
– дате, времени;
– протоколу;
– типу атаки и т. д.

Коммутаторы все активнее используются в корпоративных сетях, поскольку они обладают большей пропускной способностью по сравнению с концентраторами и защищают от атак с использованием программ-снифферов для перехвата конфиденциальной информации. Тем не менее, проблемы с применением NIDS сохраняются. Существуют коммутаторы с зеркалированием портов (SPAN-порты), которые копируют данные, проходящие через коммутатор, на выделенный порт. Теоретически, с помощью SPAN-порта возможно проверить весь поток данных, однако если объем зеркалируемого трафика превысит допустимый предел, то начинаются потери пакетов.

Существуют решения для гигабитной сети, но есть еще одна проблема – шифрование. Администраторы удаленно работают со своими системами с применением SSH или SSL, а поскольку передача данных идет в шифрованном виде, проблема использования IDS остается. Она заключается в невозможности расшифровать весь трафик и, как следствие, проверить сигнатуры атак. В ближайшем будущем практически все производители планируют доработать свои изделия для применения в гигабитной сети.

Зарубежные разработчики отмечают еще одну важную проблему – сбор информации и ее анализ. Цель решения проблемы – исключить человеческий фактор. Начаты проекты Spice и Spade, направленные на развитие технологии выявления аномальной активности, и они должны помочь в решении данной проблемы.

Системы IDS развиваются в направлении сбора и корреляции информации. При этом информация должна поступать от разнообразных источников (сенсоров). Различия между NIDS и HIDS постепенно исчезнут, и в дальнейшем будут созданы системы централизованного управления с возможностями принятия решения, что заметно снизит нагрузку на администраторов, ответственных за безопасность компьютерных сетей.

## Отечественные системы обнаружения, предупреждения и ликвидации компьютерных атак (вторжений)

При проведении сертификации ФСБ России выделяет четыре класса систем обнаружения атак (СОА) – от Г до А (от «низшего» к «высшему»).

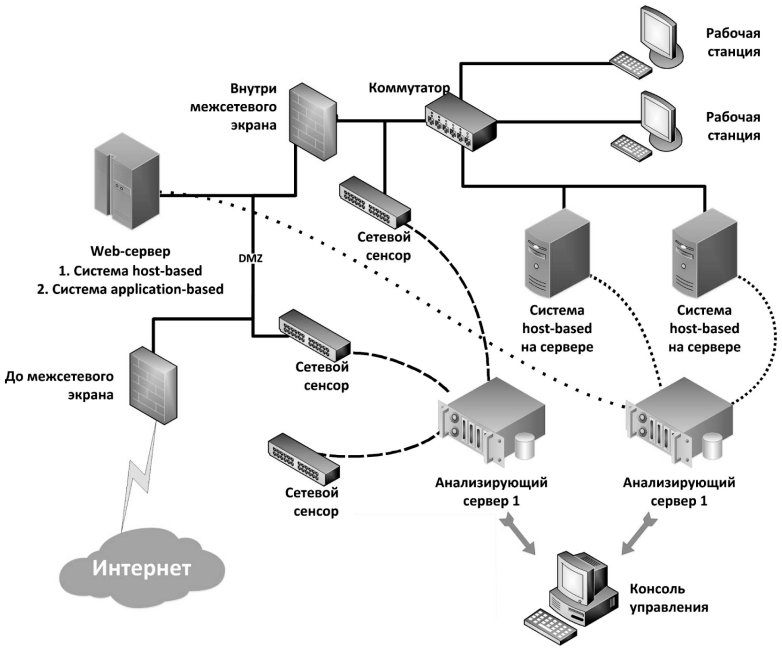


*Рис. 1. Общая схема функционирования IDS*

При проведении сертификации ФСТЭК России выделяет шесть классов систем обнаружения вторжений (СОВ), шестой класс – «низший».

Перечень СОА (СОВ), сертифицированных ФСБ или ФСТЭК России, приведен в таблице 1.

Система обнаружения компьютерных атак «Форпост» применяется в автоматизированных информационных системах (АИС) с производительностью до 1 Гбит/с, имеет механизм фильтрации событий, отображаемых в журналах СОА, и интуитивно-понятный русскоязычный графический интерфейс администрирования. Работает под управлением операционных систем Windows XP/7, Windows Server 2003/2008.

СОА «Форпост» обеспечивает генерацию табличных и текстовых отчетов на основе содержимого журналов СОА. Распределенная модульная архитектура, масштабируемость СОА «Форпост», позволяет адаптироваться под требования конкретной АИС по производительности и отказоустойчивости.

Программно-аппаратный комплекс (ПАК) «Тор» предназначен для обнаружения компьютерных атак в сетевом трафике стека протоколов TCP/IP в каналах со скоростью передачи данных до 100 Мбит/с включительно с использованием сигнатурного метода. Функционирует под управлением операционной системы Атликс-2И (ядро Linux версии 2.6.32, на базе CentOS Linux). Управление осуществляется удалённо при помощи Web-интерфейса с использованием СКЗИ AtlixGCL из состава ОС Атликс-2И.

Программно-аппаратный комплекс «ViPNet IDS» обеспечивает:

– обнаружение компьютерных атак (вторжений) на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным;

– регистрацию компьютерных атак (вторжений) в момент времени, близкий к реальному;

– отображение обобщенной статистической информации об атаках;

– журналирование обнаруженных событий и атак для последующего анализа;

– экспорт журнала атак (вторжений) в файл формата CSV для последующего анализа в сторонних приложениях;

– обновление баз решающих правил в автоматизированном режиме с сервера обновлений при предоставлении новой версии указанной базы производителем;

– механизм, обеспечивающий маскирование ПАК ViPNet IDS в составе контролируемой сети;

– выборочное использование отдельных правил обнаружения или групп правил на усмотрение администратора ViPNet IDS;

– добавление собственных правил для анализа сетевого трафика;

– выборочный контроль ресурсов сети на уровне отдельных объектов;

– регистрация, отображение и экспорт в файл формата PCAP IP-пакетов, соответствующих зарегистриро-

Таблица 1

**Перечень сертифицированных СОА (СОВ)**

| Наименование СОА (СОВ) | Организация-разработчик | Сертификат ФСБ | Сертификат ФСТЭК |
|---|---|---|---|
| Аргус, версия 1.0 | Центр Специальной Системотехники | СОА Г СФ/129-1577 | - |
| Аргус, версия 1.5 | Центр Специальной Системотехники | СОА В СФ/129-1655 | ТУ, НДВ 4 (№ 2487) |
| Детектор атак «Континент» | ООО «Код Безопасности» | - | СОВ С3, НДВ 2,МЭ (№ 3008) |
| Рубикон | Эшелон | - | ТУ, НДВ 2, МЭ (№ 2574) |
| Ручей-М | УЦ ИнформПро | СОА Г СФ/129-2212 | - |
| Тор | НТЦ Атлас | СОА Б СФ/129-1818 | - |
| Форпост, версия 2.0 | РНТ | СОА Б СФ/129-1753 | СОВ С3 (№ 2845) |
| ViPNet IDS | ИнфоТекс | СОА В СФ/129-2253 | - |

ванным событиям (атакам), для последующего анализа в стороннем программном обеспечении (ПО);

– автоматическая передача обобщенной информации о сетевых атаках (вторжениях) системе централизованного мониторинга ViPNet StateWatcher по протоколу SNMP;

– контроль целостности исполняемых и конфигурационных файлов;

– контроль целостности загружаемых баз правил обнаружения атак.

Аппаратно-программный комплекс (АПК) обнаружения компьютерных атак «Аргус» проводит анализ протоколов в реальном масштабе времени на скорости канала до 1 Гбит/сек. При использовании в организации нескольких АПК «Аргус» версии 1.5 появляется возможность анализа трафика, превышающего 1 Гбит/сек. В этом случае в одном сегменте сети устанавливается несколько АПК, данные от которых собираются и обрабатываются на сервере «Система РАМС ИБ».

Для поиска компьютерных атак АПК «Аргус» выполняет сигнатурный анализ сетевого трафика, анализ протоколов, анализ аномалий, анализ по накопленной статистике для протоколов 3–7 уровней эталонной модели взаимодействия открытых систем.

Для проведения дальнейших исследований наибольший интерес представляют изделия комплекса «Континент» компании ООО «Код Безопасности».

Система обнаружения вторжений входит в состав АПК «Континент» – изделия, предназначенного для защиты корпоративных распределенных сетей. Организация защищенной корпоративной сети с применением АПК «Континент» (вариант) представлен на рис. 2.

Обнаружение вторжений осуществляется по результатам анализа зеркального трафика, поступающего от криптошлюза или маршрутизатора.

Основным компонентом СОВ является детектор атак «Континент» (далее – ДА), который представляет собой программное средство, установленное на специализированной аппаратной платформе.

Детектор атак обеспечивает обнаружение преднамеренного несанкционированного доступа или специальных воздействий на информацию со стороны:

– внешних нарушителей, действующих из информационно-телекоммуникационных сетей;

– внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Детектор атак реализует следующие основные функции:

– сбор информации о пакетах данных;

– анализ собранной информации;

– оперативное реагирование на выявленные вторжения;

– оповещение центра управления сетью криптографических шлюзов (ЦУС) о своей активности и о событиях, требующих оперативного вмешательства в режиме реального времени;

– регистрация событий, связанных с работой ДА;

– идентификация и аутентификация администратора при запуске ДА;

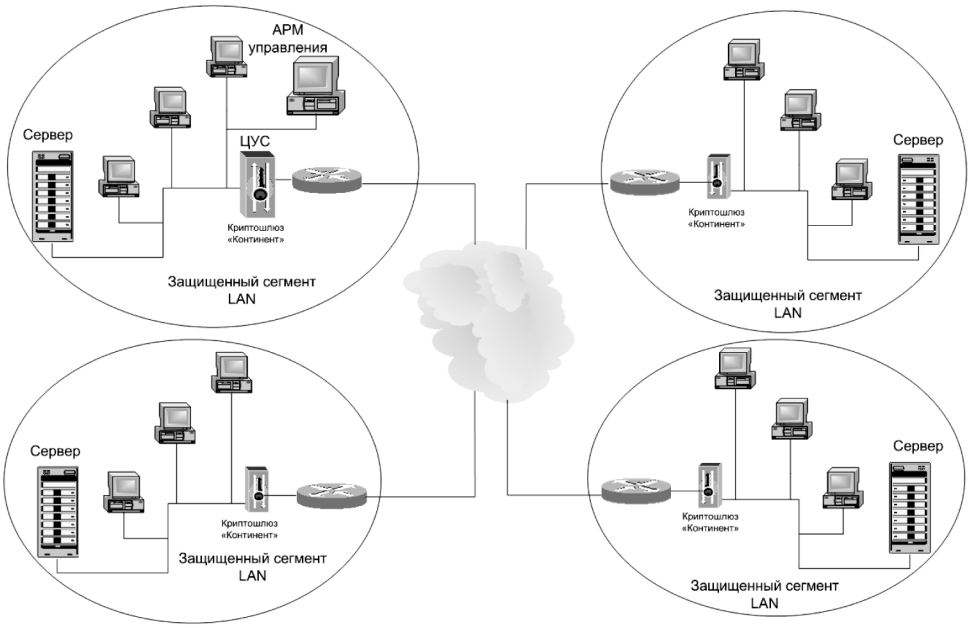


*Рис. 2. Организация защищенной корпоративной сети с применением АПК «Континент» (вариант)*

– контроль целостности программного обеспечения ДА.

Детектор атак контролирует следующие данные о сетевом трафике:

– сетевой адрес;

– используемый порт;

– значения полей сетевого пакета;

– аппаратный адрес устройства (при отсутствии сетевого адреса);

– идентификаторы протоколов;

– последовательность команд протоколов;

– размер полей пакета;

– интенсивность трафика.

Анализ данных с целью обнаружения вторжений осуществляется с использованием сигнатурного и эвристического методов.

Метод сигнатурного анализа основан на применении решающих правил, предварительно загруженных в базу данных ЦУС и постоянно обновляемых с требуемой периодичностью.

Эвристический анализ выявления аномалий сетевого трафика может применяться в дополнение к сигнатурному анализу. При этом используются настройки эвристического анализатора, заданные по умолчанию. Также предусмотрены режимы обучения эвристического анализатора на «разрешенном» или «запрещенном» трафике и возврат к исходным настройкам.

События, связанные с фунционированием ДА и обнаружением вторжений, регистрируются в его локальных журналах и средствами агента ЦУС передаются в базу данных.

Просмотр событий осуществляется в программе просмотра журналов. Кроме того, в случае обнаружения вторжения или нарушения безопасности администратору отсылается сообщение электронной почты, а в программе управления появляется визуальное отображение зафиксированного несанкционированного действия.

Возможный набор ответных действий на компьютерные атаки (вторжения) зависит от используемой системы. Например, в системе ISS RealSecure Network Sensor существуют следующие варианты автоматического реагирования на атаки:

– запись факта атаки в регистрационном журнале RealSecure;

– уведомление об атаке администратора через консоль управления средствами RealSecure;

– уведомление об атаке заинтересованных лиц по электронной почте;

– аварийный разрыв соединения с атакующим узлом;

– запись IP-пакетов, вызвавших срабатывание системы обнаружения атак (воздействий), в отдельный файл для последующего анализа;

– посылка управляющих SNMP-последовательностей.

Количество криптошлюзов в сети с одним ЦУС не превышает 500.

## Заключение

Из приведенного обзора можно сделать следующие выводы:

– в отечественных и в зарубежных СОА используются практически одни и те же принципы построения, функционирования систем и методы обнаружения атак (сигнатурный, эвристический и их комбинации);

– первичными источниками информации о компьютерных атаках являются сенсоры (с установленными на них программами агентов сети), которые выполняют такие же функции, что и детекторы атак в отечественных системах;

– от сенсоров информация о компьютерных атаках поступает на центральный анализирующий сервер, который обеспечивает хранение и обработку информации с помощью интерфейса пользователя. Сервер реализует такие же функции, что и АРМ администратора в отечественных СОА (СОВ).

Проблема обеспечения информационной безопасности может быть решена на основе разработки и упреждающего применения эффективных отечественных систем обнаружения, предупреждения и ликвидации компьютерных атак (вторжений).

Для достижения целей по защите информации необходимо сочетать правовые, организационные и технические меры. Это сочетание определяется степенью конфиденциальности защищаемой информации, характером опасности и наличием средств защиты.

## Литература

1. Указ Президента РФ от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

2. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом РФ от 09.09.2000 г. № Пр-1895.

3. Закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации».

4. Астахов, А. Актуальные вопросы выявления сетевых атак / А. Астахов, CISA // Информационный бюллетень Jet Info. – 2002. – № 3 (106). – 28 с.

5. Костров, Д. Системы обнаружения атак / Д. Костров // Byte/Россия. – 2002. – № 8. – С. 20–22, 24–26.