УДК 004.491.22

М.Е. Бурлаков

Модель многослойной универсальной системы обнаружения вторжений

Проектируется модель универсальной системы обнаружения вторжений. Вводятся требования по проектированию базы данных универсальной системы обнаружения вторжений, а также определяется общий принцип работы в многоступенчатых информационных системах и описывается процесс безотрывного обучения и тренировки. Обосновывается актуальность и новизна созданной модели.

Ключевые слова: универсальная система обнаружения вторжений; многоступенчатые информационные системы.

Под системой обнаружения вторжений (СОВ) понимается программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную / информационную систему или сеть либо несанкционированного управления ими злоумышленником. СОВ включает в себя: сенсорную подсистему, подсистему анализа, хранилище и консоль управления.

Как следует из определения, СОВ – это пассивная система. Существует множество классификаций СОВ в зависимости от области и вариантов применения в информационных системах [1]. Например, существует классификация в зависимости от использования на том или ином уровне сетевой модели *OSI* [2], на основании этого выделяют следующие типы СОВ:

1) сетевые. Например, *Snort* [3]. Уровень *OSI*: транспортный и сеансовый;

2) основанные на протоколе. Например, модуль *Nginx*. Уровень *OSI*: представление;

3) основанные на прикладных протоколах. Например, компилятор *MySQL*. Уровень *OSI*: прикладной;

4) узловые. Например, *OSSEC*. Уровень *OSI*: транспортный и сетевой;

5) гибридные. Например, *Prelude*. Уровень *OSI*: транспортный, сетевой и сеансовый.

Существенным недостатком всех современных систем обнаружения вторжений является либо их строгая направленность на решение задач в конкретном уровне сетевой модели, либо небольшая вариативность в плане работы с несколькими уровнями передачи информации [4]. Под уровнем передачи информации (УПИ) будем понимать программно-аппаратный блок, принимающий и впоследствии передающий данные другим(ому) блокам(у). В настоящее время отличительной особенностью УПИ является отсутствие универсальной программно-аппаратной реализации обнаружения вторжений в информационных системах.

В данной работе предлагается теоретическая модель универсальной системы обнаружения вторжений, которая может быть подключена к любому типу УПИ. Под универсальностью понимается единая структура СОВ, единая методика обработки данных вне зависимости от выбранного уровня передачи информации.

Теоретическая модель универсальной системы обнаружения вторжений. Основополагающим элементом универсальной системы обнаружения вторжений является база данных (БД). В предлагаемой модели с целью обеспечения проектируемой универсальности БД должна состоять из следующего набора элементов:

1. Блок хранения единого реестра срабатываний (ЕРС). ЕРС хранит в себе информацию обо всех угрозах, на которые сработали все СОВ в рамках информационной системы. Структура хранения данных в ЕРС имеет вид «Набор угроз» – «СОВ*i*», где «Набор угроз» – множество найденных угроз, СОВ*i* – *i*-я система обнаружения вторжений, перехватившая угрозу. Для дальнейшего анализа получаемых данных в предлагаемой системе ЕРС должны содержаться следующие типы сортировок:

а) сортировка по дате занесения записи, позволяющая отслеживать интенсивность детектирования угроз, поступающих на все УПИ;

б) сортировка по СОВ*i*, отслеживающая количество угроз на конкретный УПИ;

в) сортировки, определяемые оператором в зависимости от решаемой задачи.

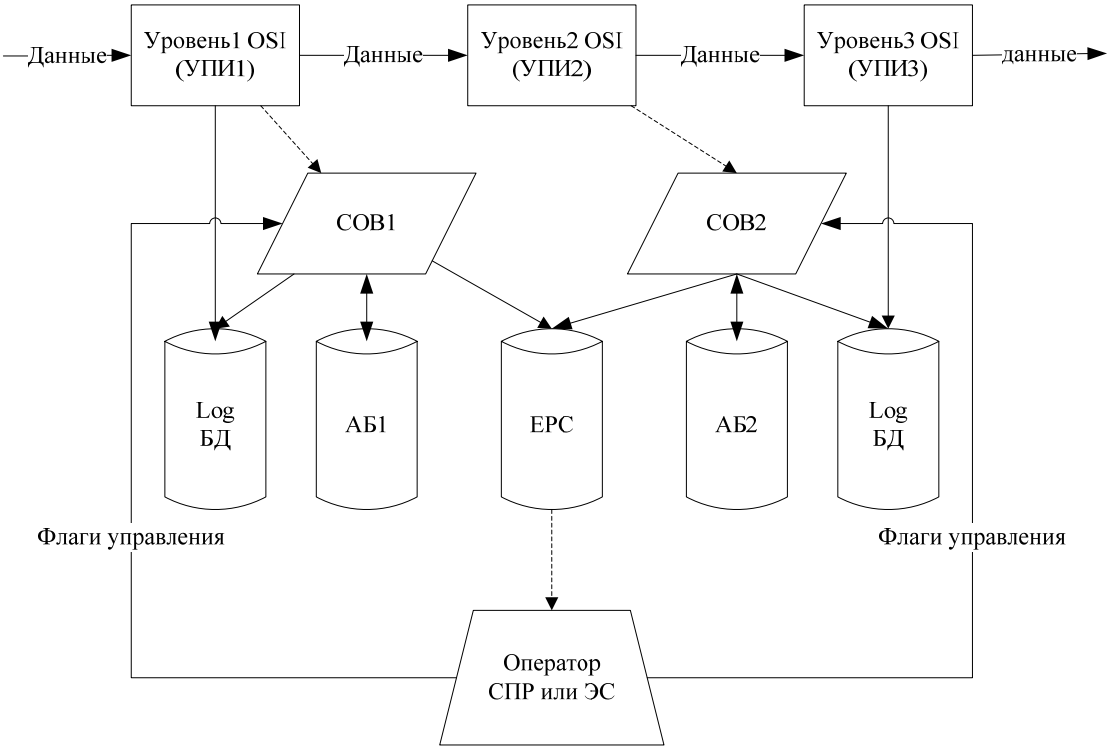
2. Блоки актуальных библиотек (АБ) по УПИ. Для каждого УПИ предполагается наличие своей библиотеки с хранимыми векторами угроз.

3. Блоки инициализационных библиотек (ИБ). Инициализационные библиотеки предполагают наличие первоначальных данных для начала работы СОВ, а также для обеспечения корректного процесса ее обучения. В предлагаемой модели ИБ – полный аналог АБ по структуре строения.

4. Блоки тренировки (ТБ). Создаются после инициализации на стороне СОВ процесса тренировки. Вся структура создания ТБ описывается в инициализационном файле (ИФ), который формируется оператором либо сторонней системой.

5. Блок логирования (*Log* блок). Данный блок отвечает за сбор потока данных. *Log* блок может как накапливать информацию, присланную с УПИ, так и информацию уже обработанную СОВ. В первом случае структура хранения данных в этом блоке эквивалентна структуре передаваемых данных в СОВ. *Log* блок может формироваться как самой СОВ, так и УПИ. Для разных систем может быть создана единая *Log* БД вида «*Log* БД УПИ» – «Тип УПИ». Наличие *Log* блока не является обязательным для УПИ.

Общая структурная модель предлагаемой универсальной системы обнаружения вторжений представлена на рис. 1. Пунктирная линия от УПИ к СОВ подразумевает возможность исключения СОВ из процесса передачи данных.



СПР – система принятия решений, ЭС – экспертная система

Рис. 1. Модель работы универсальной системы обнаружения вторжений

Рассмотрим работу предлагаемой универсальной системы обнаружения вторжений пошагово.

1. Данные поступают в уровень *OSI* (УПИ1).

2. Далее информация передается на следующий уровень УПИ2. Параллельно данные передаются в блок СОВ (СОВ1), и осуществляется запись данных в *Log* блок средствами УПИ, в случае если это предусмотрено конфигурацией работы системы.

3. Используя блок АБ (на рис. АБ1 или АБ2), СОВ принимает решение о легитимности или нелегитимности принятых данных. В случае если данные не легитимны (угроза), происходит запись в единый реестр срабатываний, который в свою очередь анализируется оператором или сторонней системой. В качестве активной сторонней системы может быть рассмотрена экспертная система (ЭС) или система принятия решений (СПР).

4. Оператор может влиять на СОВ через флаги управления. В предлагаемой модели флаги управления СОВ включают в себя:

а) флаг включения/выключения. Данный флаг позволяет включать или выключать СОВ между УПИ при анализе потока данных в информационной системе;

б) флаг обучения и тренировки. Флаг позволяет активировать режим обучения и тренировки. При активации данного режима система использует определенный конфигурационный файл (КФ), позволяющий автоматически формировать среду обучения и тренировки. Данные для последующего обучения и тренировки берутся из *Log* блока. Также создаются инициализационные и тренировочные блоки (запись данных), а единый реестр срабатываний используется только для чтения с целью дальнейшего анализа эффективности СОВ. Обучение и тренировка СОВ также описываются КФ, созданным оператором, либо сторонней системой.

Режим обучения и тренировки универсальной системы обнаружения вторжений. Для начала корректной работы СОВ необходимы ее предварительное обучение и тренировка. Введем ряд определений элементов обучения и тренировки:

БД конфигураций – база данных конфигураций с типом хранения вида «конфигурация» – «СОВ», позволяющая сохранять конфигурацию СОВ в определенный момент времени. В рамках процесса обучения и тренировки СОВ используется оператором либо другой системой с целью дальнейшего анализа наиболее оптимальных конфигураций СОВ.

Загрузчик конфигураций (ЗК) – программно-аппаратное решение, обеспечивающее подготовку конфигураций для СОВ с последующим ее обновлением. Загрузчик конфигураций обладает функцией считывания текущей конфигурации СОВ с возможностью последующего ее сохранения в БД конфигураций.

Конфигурационный файл (КФ) – файл с определенной структурой, с помощью которого производится управление выбранной СОВ. Под управлением СОВ понимается либо определение и инициализация режима обучения и тренировки, либо текущая настройка его работы.

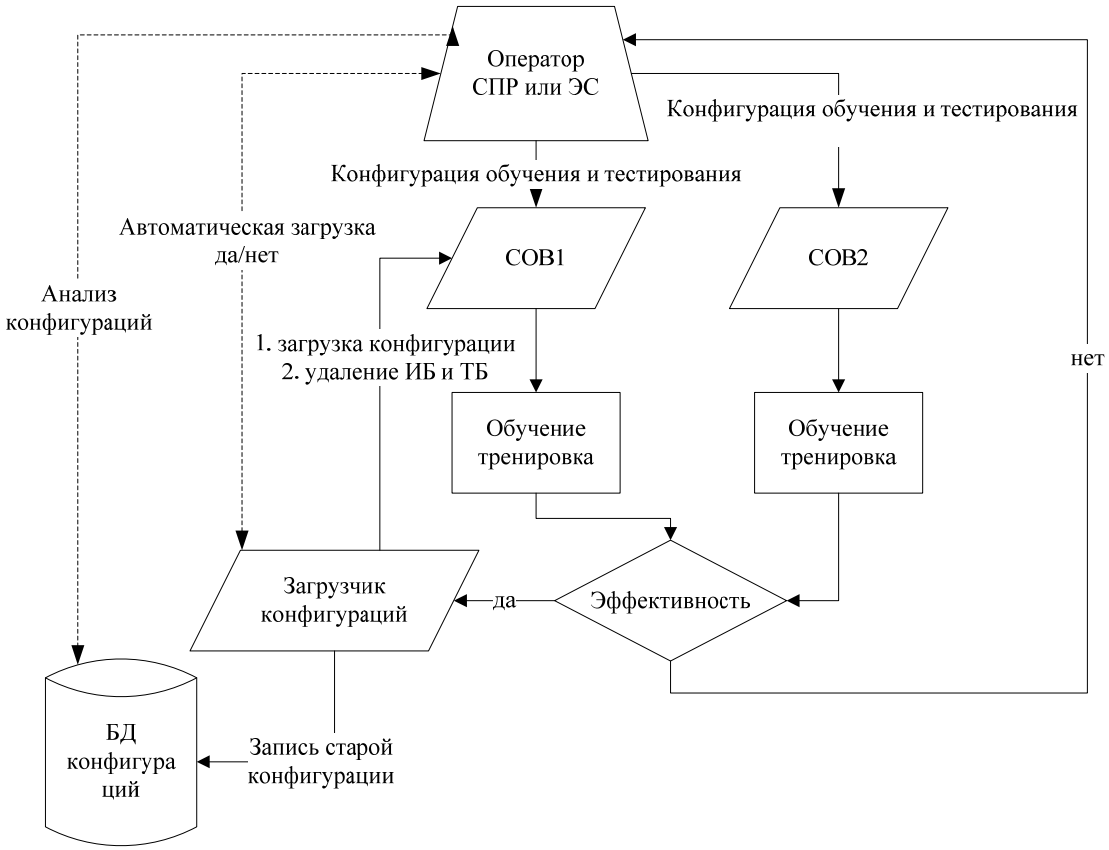


Рис. 2. Упрощенная структурная модель обучения и тренировки функционирующей СОВ

Структурная схема обучения и тренировки двух СОВ в рамках работающих УПИ представлена на рис. 2. На рис. 2 представлен только участок информационной системы с конечным числом блоков УПИ и соответствующим им СОВ. В общем случае количество блоков СОВ в рамках ИС не регламентируется.

Рассмотрим процесс обучения и тренировки системы обнаружения вторжений пошагово.

1) включение флага тренировки;

2) загрузка конфигурационного файла обучения и тренировки в СОВ и создание инициализационного и тестового блоков;

3) обучение и тренировка;

4) определение меры эффективности:

а) «Эффективно». Новые параметры отправляются в загрузчик конфигураций. Параллельно в базе данных конфигураций сохраняется старая конфигурация СОВ. Загрузчик конфигураций в зависимости от определенных настроек либо оператором, либо автоматически загружает новые параметры в рабочую версию СОВ;

б) «Не эффективно». Отчет отправляется либо оператору, либо в другую систему для последующего анализа.

В предложенной модели конфигурационный файл процесса обучения и тренировки универсальной системы обнаружения вторжений имеет следующие параметры: параметр настройки формирования инициализационного блока (ИБ) на основе блока актуальных библиотек (АБ), параметр настройки формирования тестового блока (ТБ) и параметр работы процесса обучения и тренировки СОВ с использованием единого реестра срабатываний и *Log* блока.

Детальный процесс обучения для системы обнаружения вторжений представлен на рис. 3.

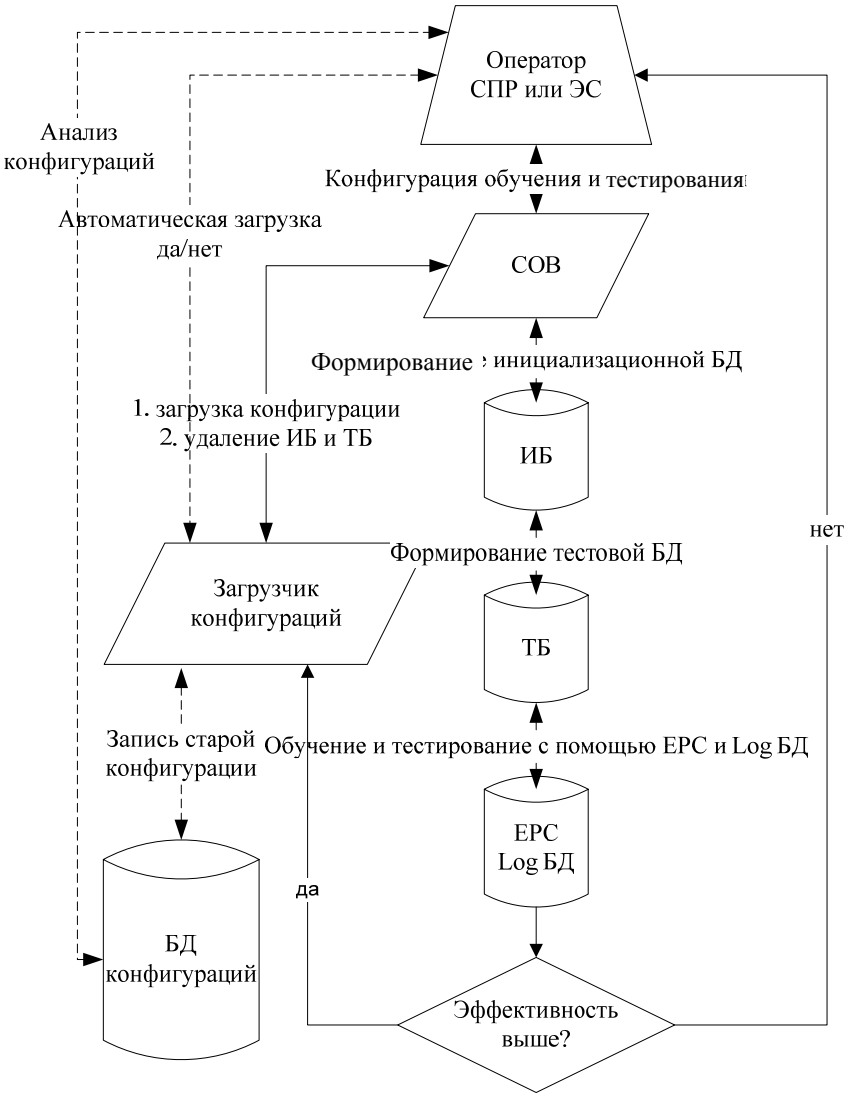


Рис. 3. Подробная модель обучения и тренировки универсальной СОВ

Рисунок 3 отличается от рис. 2 в части детального описания процесса обучения и тестирования, которые состоят из следующих шагов:

1) включение флага тренировки;

2) формирование инициализационного блока (ИБ);

3) формирование тестового блока (ТБ);

4) обучение и тестирование СОВ с использованием единого реестра срабатываний и Log базы данных;

5) оценка эффективности работы.

В результате представленных выше пошаговых алгоритмов, реализована теоретическая модель универсальной системы обнаружения вторжений, включающая в себя процессы обучения и тренировки. Предложенная модель позволяет универсализировать использование системы обнаружения вторжений в разных типах УПИ в отличие от известных моделей, которые подразумевают выполнение конкретных задач.

Заключение. В данной статье была предложена теоретическая модель универсальной системы обнаружения вторжений. К основным плюсам описанной системы можно отнести:

Динамичность и актуальность. За счет наличия единого реестра срабатываний и процесса безотрывного обучения и тренировки СОВ обеспечиваются актуальность данных и ее постоянная адаптация к текущей среде передачи информации.

Независимость. За счет наличие флага управления «включение/выключение» СОВ и параллельности обработки данных с УПИ предложенная модель обеспечивает независимость и параллельность к информационной системе.

Унификация. Обеспечивается за счет универсальности хранения (баз данных) и обработки информационных потоков СОВ.

К потенциальному недостатку можно отнести возможную большую нагрузку на блок реализации СОВ. Недостаток может быть исключен путем внедрения процесса распараллеливания комплекса СОВ на многопроцессорных информационных системах.

Литература

1. Бурлаков М.Е. Аудит безопасности локальной вычислительной сети с помощью динамической системы на нейронах с реакцией на последовательности / М.Е. Бурлаков, М.Н. Осипов // Матер. XIII Междунар. науч.-практ. конф. «ИБ-2013». – Таганрог: Изд-во ЮФУ, 2013. – Ч. 1. – С. 85–91.

2. ГОСТ Р ИСО/МЭК 7498-1–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Введ. 1999-03-18. – М.: Гостстандарт, 2006. – 62 с.

3. Everett F. Snort IDS and IPS Toolkit / F. Everett, C. James, M. Jonkman. – Kohlenberg: Syngress, 2007. – 41 p.

4. Бурлаков М.Е. Метод фильтрации входящего трафика на основе двухслойной рекуррентной нейронной сети // Ползуновский вестник. – 2012. – № 3/2. – С. 215–219.

Бурлаков Михаил Евгеньевич
Аспирант каф. безопасности информационных систем Самарского государственного университета
Тел.: 8-929-703-33-38
Эл. почта: knownwhat@gmail.com

Burlakov M.E.

The common model of intrusion detection system

A common model of intrusion detection system (IDS) is described in the article. There are requirements for designing a database of IDS, as well as the general principle of operations are determined in multi-information systems and there is description of the process of education and training IDS. The usefulness of model is justified.

Keywords: universal intrusion detection system, multi-information systems.