§7 МОДЕЛИ И МЕТОДЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Заводцев И. В., Гайнов А. Е.

РАЗРАБОТКА МЕХАНИЗМОВ СБОРА И ПРЕОБРАЗОВАНИЯ ФОРМАТА ПРЕДСТАВЛЕНИЯ ИСХОДНОЙ ИНФОРМАЦИИ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *В функциональной структуре СУИИБ существенное значение имеют механизмы сбора и преобразования формата представления исходной информации. Поэтому в работе рассматриваются вопросы разработки модуля трансляции событий, который обеспечит слияние регистрационных событий в одну точку. Причем важным также является возможность реализации передачи исходных данных от одиночных сенсоров в консолидированную БД системы корреляции. Для этого необходима разработка механизма агрегации данных с их последующей нормализацией и приоретизацией, что обеспечит сжатие исходных данных для последующего принятия решения о наличии/отсутствии инцидента информационной безопасности за текущий промежуток времени. Проведена разработка математического аппарата для модуля трансляции событий перспективных СУИИБ, который обеспечит слияние регистрационных событий из многих источников в одну точку. В работе предложен механизм сбора и преобразования формата представления исходной информации, включающий: процедуру преобразования данных перед транспортировкой за счет присвоения буквенных или цифровых идентификаторов полям журналов регистрации построчно и разбиении этих идентификаторов на группы; процедуры категоризации и приоритезации; алгоритм агрегирования данных о событиях, основанный на расчете выборочного коэффициента корреляции признаков элементарных событий между собой.*

Ключевые слова: *события информационной безопасности, информационная безопасность, управление инцидентами, СУИИБ, извлечение данных, журналы регистрации, нормализация данных, категоризация событий, приоритезация событий, фильтрация данных*

Современные информационные системы, как правило, имеют достаточно развитую и сложную структуру, десятки типов разнородных систем, соответственно, большой объем

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010

При цитировании этой статьи сноска на DOI обязательна

поступающей информации, что делает анализ всего потока событий и своевременное реагирование на него зачастую критичным [1]. Кроме того, существует и необходимость хранения всей информации о произошедших событиях, как для статистики, так и для проведения расследований или выявления причин сбоев, спустя длительное время [2]. Все это делает задачу сбора и анализа событий безопасности не тривиальной.

Для эффективной обработки поступающего потока событий информационной безопасности (ИБ) средствам защиты необходимо проводить: нормализацию и фильтрацию данных, агрегацию, корреляцию и приоритезацию событий безопасности. Что требует внедрения специальных технологий, определяя новые требования к научно-методическому аппарату разработки компонентов систем управления инцидентами информационной безопасности (СУИИБ) [3-5].

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

Извлечение данных

В функциональной структуре перспективных СУИИБ существенное значение имеют механизмы сбора и преобразования формата представления исходной информации. Поэтому необходима разработка модуля трансляции событий, который обеспечит слияние регистрационных событий в одну точку [3, 5].

При этом процесс консолидации реализует слияние регистрационных событий из многих источников в одну объединенную точку. На этом уровне должна обеспечиваться защита и целостность исходных данных для корреляции – путем их шифрования и верификации с помощью цифровых сигнатур. Т.е. необходимо реализовать передачу исходных данных от одиночных сенсоров в консолидированную базу данных системы корреляции.

Источниками информации для анализа СУИИБ, в общем случае, являются журналы различных компонент информационной системы: операционных систем, прикладного и общего программного обеспечения, а также средств защиты информации и др. Такие журналы содержат информацию о событиях ИБ, информация о которых представляет собой совокупность значений нескольких признаков.

В настоящей работе единичную запись в журнале регистрации будем считать *элементарным событием*, так как для разрабатываемой системы важной является возможность выбора элементарных событий при начальной настройке системы. Причем, в зависимости от решаемых задач, должна быть реализована еще и возможность сокращения множества анализируемых событий.

Так как большинство журналов имеют различный формат, то приведение данных к *единому виду* должно осуществляться специализированным агентом сбора этих данных. Основной задачей агента является сбор данных из журналов конкретного узла автоматизированной системы и отправка их в модуль преобразования данных. Агент представляет собой специализированное программное обеспечение, отдельно устанавливаемое на нужный хост, и в режиме реального времени осуществляющее считывание из журналов релевантной информации.

Существует два основных пути обмена данными между агентами и модулем преобразо-

DOI: 10.7256/2305-6061.2015.1.14010
При цитировании этой статьи сноска на DOI обязательна

вания данных: стратегия «втягивания» и стратегия «выталкивания».

Первая заключается в том, что модуль преобразования данных отправляет запрос агентам на получение данных с некоторой периодичностью. Агент, получив запрос, отправляет накопленные к этому моменту обновления журналов.

Эта модель эффективна от «перегрузки» входящим трафиком: как только принимающая сторона обработает очередную порцию данных, будет отправлен запрос на получение следующей.

Однако в этом случае крайне неэффективно используется канал передачи данных: если какой-то хост информационной системы не имеет высокой нагрузки, то модуль обработки данных будет запрашивать данные с такого хоста чаще, чем те будут появляться в журналах его безопасности.

Вторая стратегия, напротив, предполагает отправку новых данных по инициативе агента сразу же после их появления в журнале (в целях оптимизации агентом накапливается некоторый объем данных для передачи в буфер).

Здесь решается проблема неэффективного использования канала передачи данных, но возможна ситуация «перегрузки» данными уже принимающей стороны.

Преобразование данных перед транспортировкой

В общем случае, задача транспортировки состоит в безопасной передаче исходных данных от агентов ИС в модуль преобразования данных.

Так как большинство журналов регистрации, предоставляющих данные для последующей обработки, хранят их в строковом формате, то для последующей обработки средствами СУИИБ необходимо задать правила преобразования данных о события ИБ в единый формат, т.е. обеспечить нормализацию. Наиболее целесообразно использовать числовой формат, что позволит привести данные к единым показателям значимости событий, исключить противоречивость в хранении данных, а также сократить затраты при использовании математических методов обработки «сырых» данных.

Для этого рассмотрим типовые журналы регистрации, с которыми приходится работать специалистам по защите информации.

В ОС Windows 7 инфраструктура, обеспечивающая регистрацию событий, включает следующие основные журналы регистрации (на самом деле их гораздо больше, но для имитационного моделирования следует ввести ограничения) [6].

Безопасность – хранит события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам. По умолчанию – в %SystemRoot%\System32\Winevt\Logs\Security.Evtx.

Установка – в этот журнал записываются события, возникающие при установке и настройке операционной системы и ее компонентов. По умолчанию размещается в %SystemRoot%\System32\Winevt\Logs\Setup.Evtx.

Система – хранит события операционной системы или ее компонентов, напри-

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010

При цитировании этой статьи сноска на DOI обязательна

мер неудачи при запусках служб или инициализации драйверов, общесистемные сообщения и прочие сообщения, относящиеся к системе в целом. Помещается в %SystemRoot%\System32\Winevt\Logs\System.Evtx.

Пересылаемые события – если настроена пересылка событий, в этот журнал попадают события, пересылаемые с других серверов. Помещается в %SystemRoot%\System32\Winevt\Logs\ForwardedEvents.Evtx.

События оборудования – если настроена регистрация событий оборудования, в этот журнал записываются события, генерируемые устройствами – в %SystemRoot%\System32\Winevt\Logs\HardwareEvent.Evtx.

При чем, все события в журналах отражаются в двух форматах: стандартном текстовом формате и формате XML. Оба формата предоставляют одну и ту же информацию, но каждый может использоваться в разных целях. Стандартный текстовый вид предоставляет вид, дающий подробности о событии, как показано на рисунках 1 и 2.

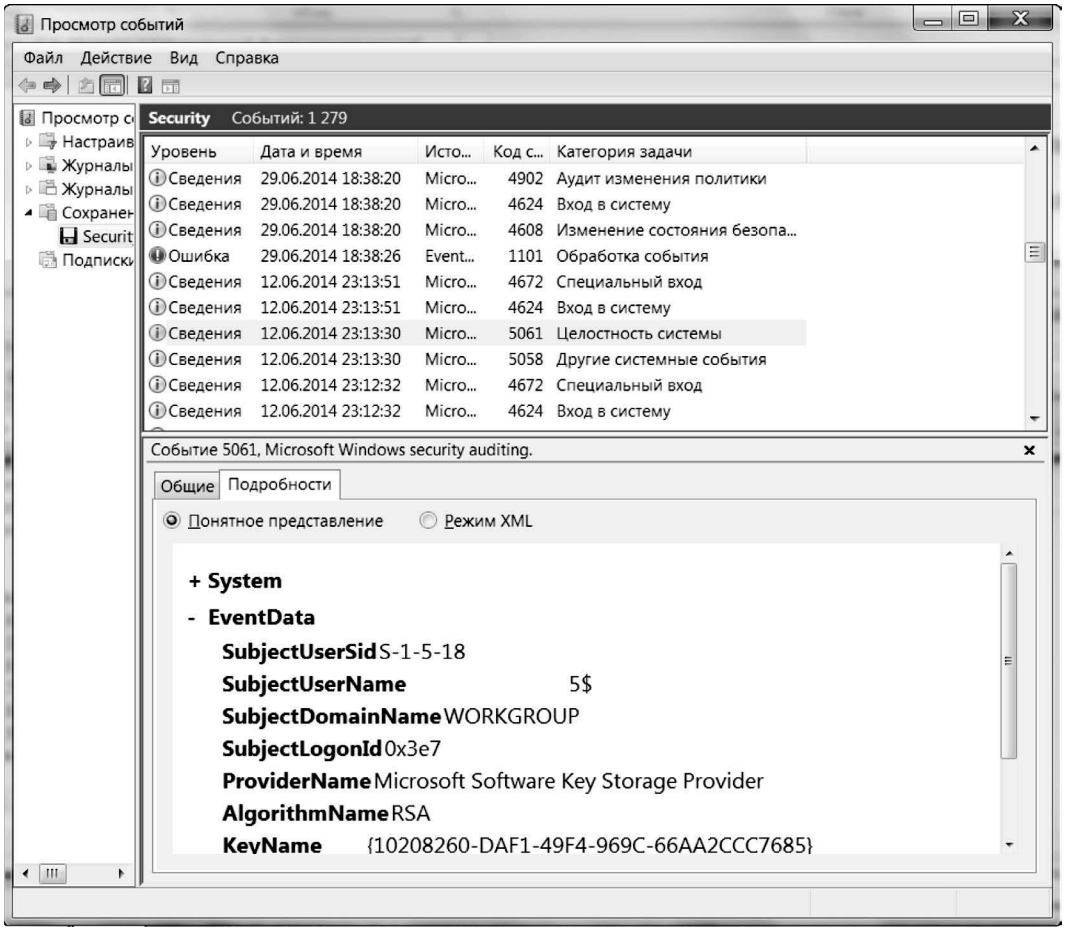

Рисунок 1 – Текстовый формат журнала Security.Evtx

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010
При цитировании этой статьи сноска на DOI обязательна

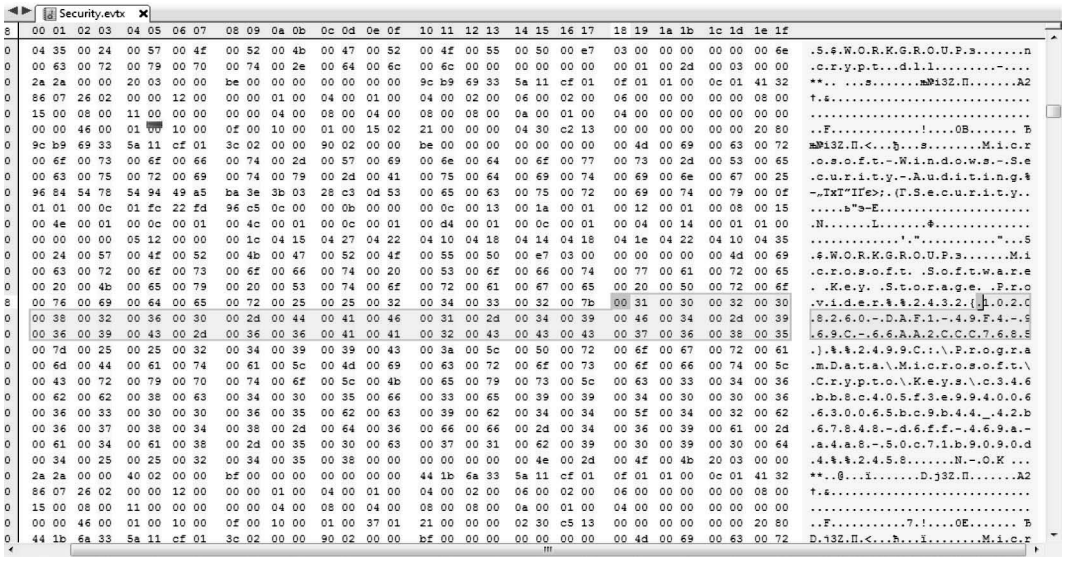

Рисунок 2 – Тот же журнал Security.Evtx, но – в редакторе шестнадцатеричных и бинарных файлов

В тоже время данные о событии, соответствующие XML-схеме (рисунок 3), позволяют не только получить доступ к XML-коду любого события, но и создавать основанные на XML запросы для получения данных из этих журналов.

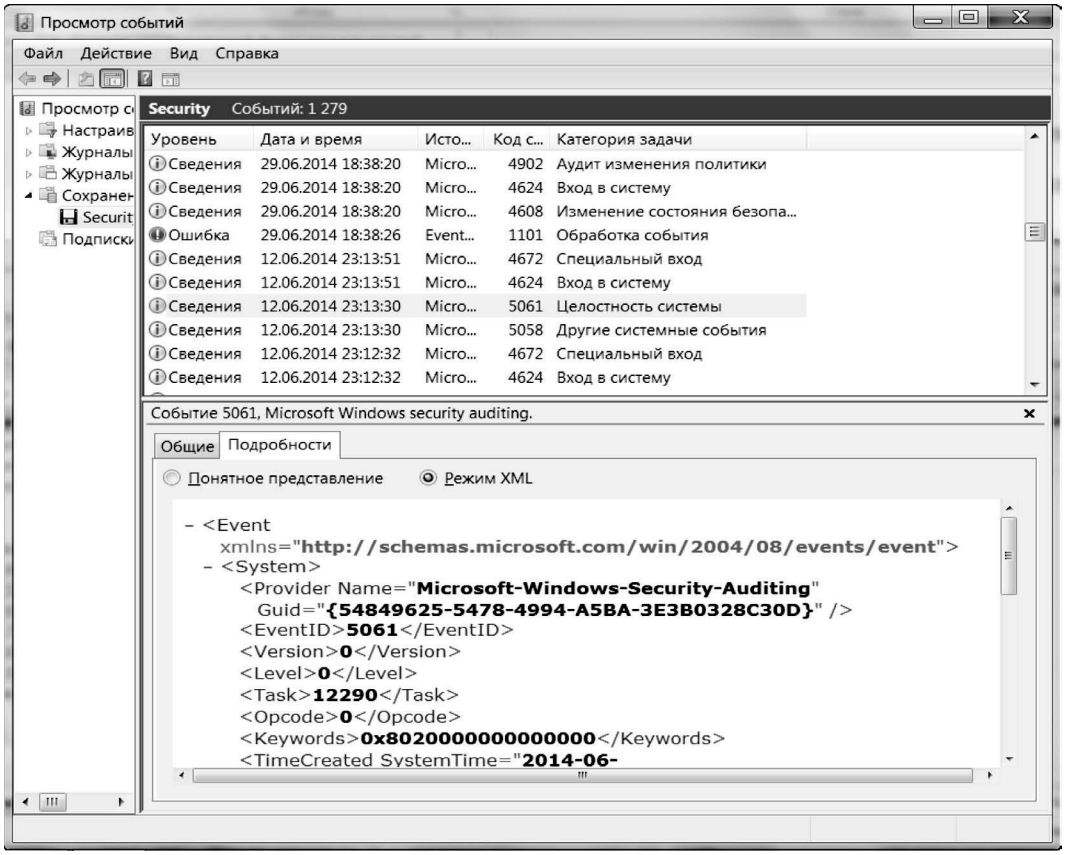

Рисунок 3 – XML-формат журнала Security.Evtx

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010

При цитировании этой статьи сноска на DOI обязательна

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

Кроме того, XML-вид журналов предоставляет формат, который можно использовать в командных сценариях (программах, PowerShell и т.д.), что целесообразно применять при экспортировании данных и последующей работе с ними на основе языка командных сценариев.

Одновременно специалист по защите информации вынужден анализировать и большое количество специализированных журналов (логов), которые генерируются различными средствами защиты информации.

Особенностью таких журналов является их разноплановость, так как каждый вендор реализует свой подход к хранению и обработке «сырых» данных. Поэтому в работе рассматриваются типовые журналы СЗИ, которые хранят данные в строковом формате: средства антивирусной защиты Dr.Web (рисунок 4-5).

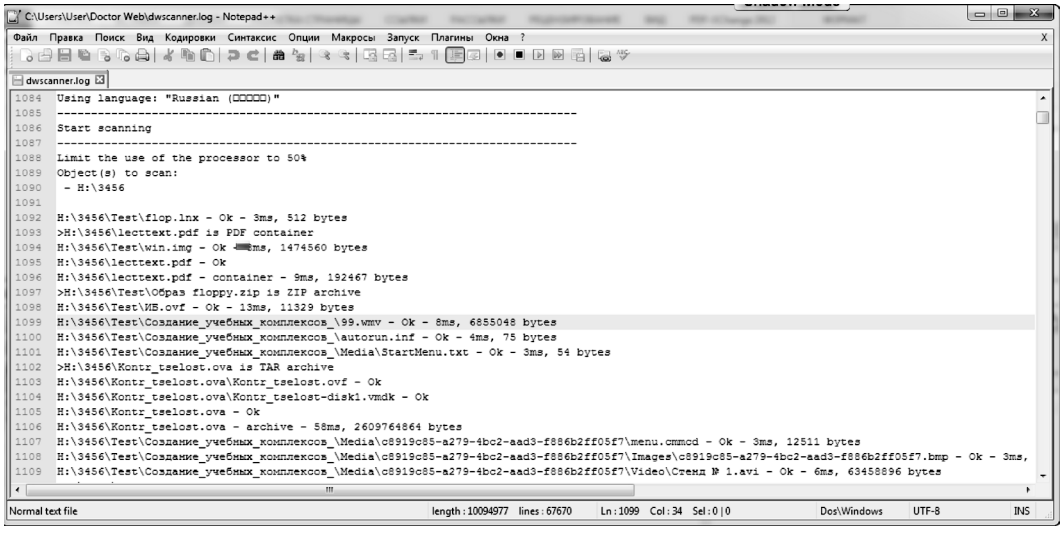

Рисунок 4 – Текстовый формат log-журнала Dr.Web

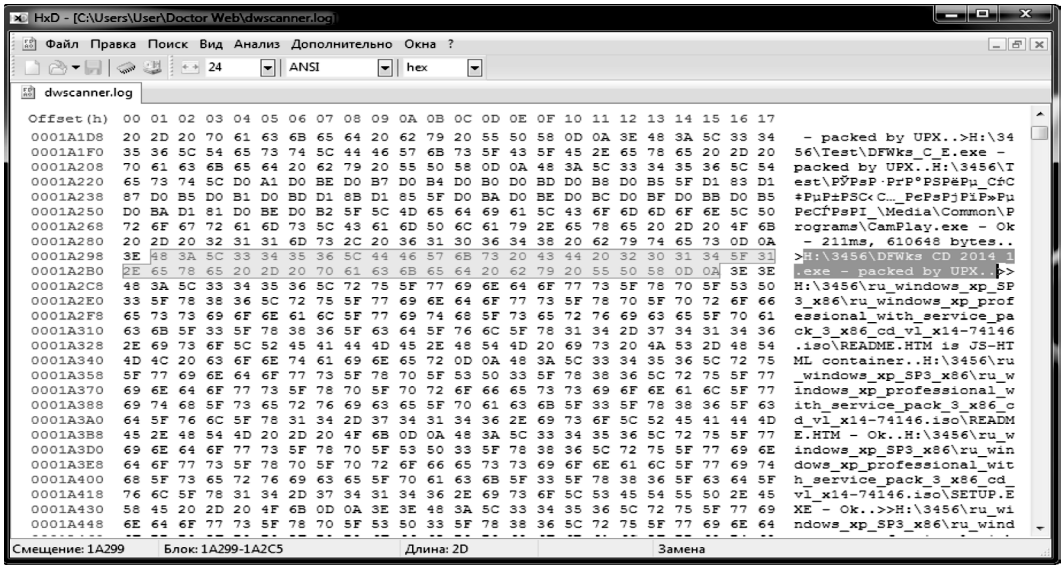

Рисунок 5 – Бинарный формат log-журнала Dr.Web

DOI: 10.7256/2305-6061.2015.1.14010

При цитировании этой статьи сноска на DOI обязательна

Нормализация данных

В настоящей работе для преобразования данных перед транспортировкой предлагается реализовать следующий *алгоритм нормализации*.

Пусть каждая строка журнала будет представлять отдельное событие, которому сопоставляется набор числовых признаков.

Первоначально производится разбиение полей строк журналов на две группы:

- в первую группу относятся признаки, множество значений которых может быть сколь угодно велико (например, Ф.И.О. пользователя, время и др.).
- во вторую – записи, которые несут в себе информацию о каком-либо действии: внешнем, со стороны пользователя или системы. При чем необходимо выделить все виды возможных типов записей и заранее пронумеровать их (например, буквами алфавита: A, B, C и т.д. – рисунок 14).

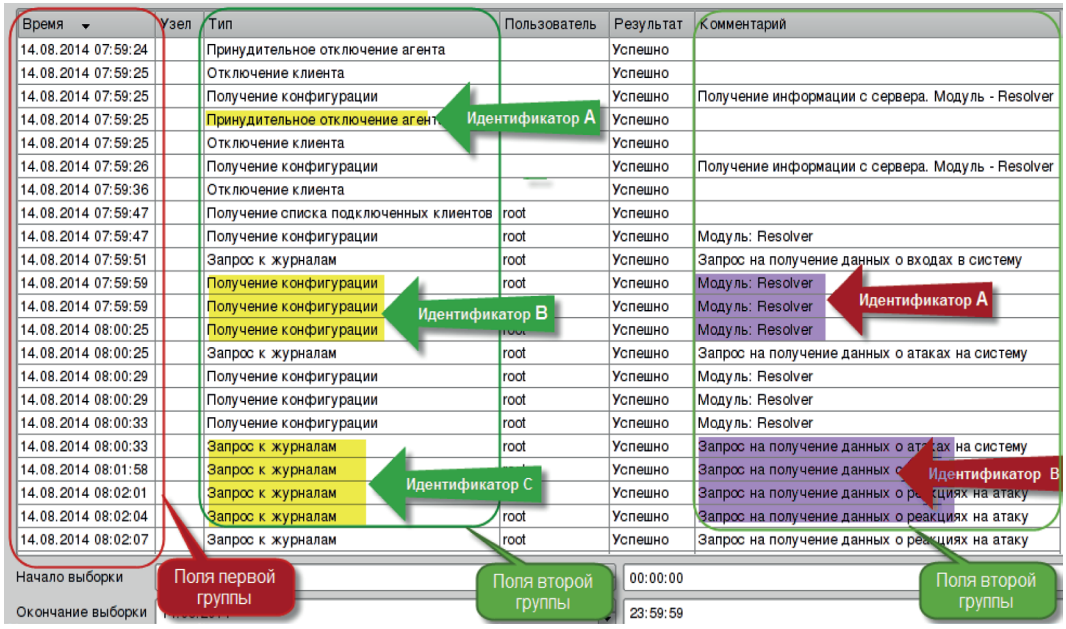

Рисунок 14 – Разбиение полей строк log-журналов на две группы

Далее производится кодирование каждой строки журнала:

- поля из первой группы нумеруются порядковыми номерами (либо игнорируются, если они могут быть отброшены на этапе фильтрации как не коррелирующие с целевой переменной).
- для кодирования полей из второй группы необходимо определить, к какому из заранее определенных типов (A, B, C) она относится, и, тогда соответствующему полю журнала, отвечающему за принадлежность записи к данному типу, присваивается значение – 1, остальным – 0. Например, в таблице ниже представлена запись журнала с информацией типа B (таблица 1).

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010

При цитировании этой статьи сноска на DOI обязательна

Таблица 1 – Присвоение идентификаторов при кодировании полей второй группы.

Идентификатор A	Идентификатор B	Идентификатор C	...
0	1	0	...

В качестве примера рассмотрим журналы ОС Windows 7:

Поле второй группы *Ключевые слова* – набор категорий или меток, которые могут использоваться для фильтрации или поиска событий. Например, для журнала «Безопасность» данное поле включает два показателя «Аудит успеха» и «Аудит отказа». Тогда таблица идентификаторов будет иметь вид, представленный в таблице 2.

Таблица 2 – Присвоение идентификаторов при кодировании поля Ключевые слова журнала Security.Evtx.

Идентификатор события	Идентификатор A	Идентификатор B
Аудит успеха	+	–
Аудит отказа	–	+

А кодировка матрицы событий в данном журнале приобретет вид:

для аудита успеха = [1, 0]; для аудита отказа = [0, 1].

Поле второй группы *Категория задачи*. Для журнала «Безопасность» данное поле включает несколько показателей:

«Вход в систему» – обычный вход, либо интерактивный, либо сетевой;

«Вход в систему*» – вход в систему с явным указанием учетных данных;

«Специальный вход в систему» – вход в систему с указанием явных привилегий;

«Выход из системы» – выход из системы.

Тогда таблица идентификаторов будет иметь вид, представленный в таблице 3. А кодировка матрицы событий в данном журнале приобретет вид: для входа в систему – [1, 0, 0, 0]; для специального входа в систему – [0, 0, 1, 0] и т.д.

Перед дальнейшей обработкой данных необходимо провести *категоризацию событий*, которая разбивает события ИБ на группы, например, по 6 различным критериям: Объект (object), Поведение (Behavior), Последствия (Outcome), Технология (Technique), Группа устройств (Device Group), Важность (Significance).

Таблица 3 – Присвоение идентификаторов при кодировании поля Категория задачи журнала Security.Evtx.

Идентификатор события	Идентификатор A	Идентификатор B	Идентификатор C	Идентификатор D
Вход в систему	+	–	–	–
Вход в систему*	–	+	–	–
Специальный вход в систему	–	–	+	–
Выход из системы	–	–	–	+

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010
При цитировании этой статьи сноска на DOI обязательна

Далее выполняется *приоритезация*, т.е. автоматическое присваивание событиям ИБ соответствующего уровня события. Приоритезация производится по четырем составляющим:

1. Доверие к ресурсу (Model confidence) – показатель, основанный на данных СУИИБ о уязвимостях ресурса, об открытых портах, об установленных обновлениях и т.д. Диапазон параметра целесообразно установить от 0 до 10.
2. Критичность ресурса (Asset Critycaly) – важность реализуемых в СУИИБ действий. Например, серверу баз данных может быть присвоено максимальное значение важности, а серверу, выполняющему роль тестового – значение равное ¼ от максимального. Диапазон параметра целесообразно установить от 0 до 10.
3. Релевантность (Relevance) – сопоставление защищенности ресурса ИС от различных угроз безопасности тому виду события ИБ, которое нацелено на конкретный вид угроз. Диапазон параметра тоже можно установить от 0 до 10.
4. Строгость (Severity) – проверка наличия зафиксированных ранее событий ИБ, относящихся к непосредственно к данному ресурсу, т.е. выявление цикличности (повторяемости) действий злоумышленника. Например, не осуществилось ли ранее сканирование портов. Диапазон параметра также можно установить от 0 до 10.

Таким образом, итоговое значение данных составит нормированное значение отношения суммы всех параметров приоритезации k-го хоста H_k к сумме их максимальных значений для отдельного хоста:

$$Prio(H_k) = \frac{ModConf(H_k)+AsCrit(H_k)+Rel(H_k)+Sev(H_k)}{Prio(H)_{max}}, \quad (1)$$

где H_k – хост в составе информационной системы с k-ым порядковым номером, $k = \overline{1, M}$.

Проведение категоризации и приортезации данных о событиях ИБ необходимо для привязки данного события ИБ к моделям защищенности ИС и уязвимостей ПО, то есть для определения уровня уязвимости и логического целеположения атакуемого ресурса или хоста в ИС.

Фильтрация данных

Следующим этапом преобразования данных является фильтрация, которая заключается в удалении избыточных событий из поступающих в систему данных. Т.е. подсистема фильтрации СУИИБ должна обеспечивать сокращение набора данных для ускорения работы программы корреляции. Сокращение данных может быть проведено через сжатие данных, стирание дублирующих наборов, фильтрацию некоторой не представляющей особой важности информации, комбинирование похожих событий воедино и т.п. События, поступающие от различных источников, исследуются на предмет дублирования информации и избыточные данные должны удаляться.

Правила фильтрации задаются администратором СУИИБ в соответствии с заданной политикой безопасности. Для успешного развертывания СУИИБ и поддержания ее эффективного функционирования требуется проводить регулярный анализ политики

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010

При цитировании этой статьи сноска на DOI обязательна

конфигурации всех сетевых устройств ИС. Такой анализ позволяет выявить и разрешить различные конфликты и аномалии в политиках, которые могут привести к серьезным нарушениям безопасности, таким как блокирование легитимного трафика, разрешение нежелательного трафика, а также небезопасные передачи данных.

Одним из методов, позволяющим снизить риски является метод «проверки на модели» для верификации правил фильтрации. Преимуществами данного метода являются его высокий уровень абстракции при представлении данных, что позволяет построить неперегруженную модель сложной ИС, выделяя лишь некоторые важные для верификации правил фильтрации функции, относящиеся к обработке запрашиваемого трафика. Кроме того метод «проверки на модели» позволяет исследовать динамическое поведение системы, не включаясь в ее рабочий процесс.

Основными входными данными в предлагаемой методике являются описания правил фильтрации политики на языке описания политики (ЯОП) и конфигурации ИС на языке описания системы (ЯОС), а также выявляемые аномалии фильтрации.

Результаты

В настоящей работе предложен механизм сбора и преобразования формата представления исходной информации, включающий:

- процедуру преобразования данных перед транспортировкой (нормализации) за счет присвоения буквенных или цифровых идентификаторов полям журналов регистрации построчно и разбиении этих идентификаторов на группы – в зависимости от значимости для дальнейшей обработки;
- процедуры категоризации и приоритезации, которые позволят в дальнейшем учитывать «вклад» тех или иных «сырых» данных в оценку значимости всей картины инцидентов ИБ в информационной системе;
- алгоритм агрегирования данных о событиях, основанный на расчете выборочного коэффициента корреляции признаков элементарных событий между собой.

Работа выполнена при поддержке «ИнфоТеКС Академия 2013-2014».

Библиография :

1. ГОСТ Р 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
2. Аналитический отчет «Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств» (по материалам Интернет-изданий за 2008-2010 гг.) М. : НТЦ «Станкоинформзащита» [Электронный ресурс] Режим доступа: http://itdefence.ru

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010
При цитировании этой статьи сноска на DOI обязательна

3. Котенко, И. В. Построение системы интеллектуальных сер-висов для защиты информации в условиях кибернетического противоборства / И.В. Котенко, И.Б. Саенко // Труды СПИИРАН. СПб.: Наука, 2012. Вып. 3(22). С.84–100.
4. Котенко, И. В. Применение технологии управления инфор-мацией и событиями безопасности для защиты информации в критически важных инфраструктурах / И.В. Котенко, И.Б. Саенко, О.В. Полубелова, А.А. Чечулин // Труды СПИ-ИРАН. СПб.: Наука, 2012. Вып. 1(20). С.27–56.
5. Заводцев, И. В. Методы и способы управления инцидентами информационной безопасности : Математические методы и информационно-технические средства / И.В. Заводцев, А.Е. Гайнов // материалы IX Всерос. науч.-практ. конф., 21–22 июня 2013 г. – Краснодар: Краснодар. ун-т МВД России, 2013. – 366 с.
6. Просмотр событий Windows [Электронный ресурс] – Режим доступа: http://windows.microsoft.com/ru-ru/windows/what-information-event-logs-event-viewer#1TC=windows-7

References:

1. GOST R 18044-2007. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment intsidentov informatsionnoi bezopasnosti.
2. Analiticheskii otchet «Obzor intsidentov informatsionnoi bezopasnosti ASU TP zarubezhnykh gosudarstv» (po materialam Internet-izdanii za 2008-2010 gg.) M. : NTTs «Stankoinformza-shchita» [Elektronnyi resurs] Rezhim dostupa: http://itdefence.ru
3. Kotenko, I. V. Postroenie sistemy intellektual'nykh ser-visov dlya zashchity informatsii v usloviyakh kiberneticheskogo protivoborstva / I.V. Kotenko, I.B. Saenko // Trudy SPIIRAN. SPb.: Nauka, 2012. Vyp. 3(22). S.84–100.
4. Kotenko, I. V. Primenenie tekhnologii upravleniya infor-matsiei i sobytiyami bezopasnosti dlya zashchity informatsii v kriticheski vazhnykh infrastrukturakh / I.V. Kotenko, I.B. Saenko, O.V. Polubelova, A.A. Chechulin // Trudy SPI-IRAN. SPb.: Nauka, 2012. Vyp. 1(20). S.27–56.
5. Zavodtsev, I. V. Metody i sposoby upravleniya intsidentami informatsionnoi bezopasnosti : Matematicheskie metody i informatsionno-tekhnicheskie sredstva / I.V. Zavodtsev, A.E. Gainov // materialy IX Vseros. nauch.-prakt. konf., 21–22 iyunya 2013 g. – Krasnodar: Krasnodar. un-t MVD Rossii, 2013. – 366 s.
6. Prosmotr sobytii Windows [Elektronnyi resurs] – Rezhim dostupa: http://windows.microsoft.com/ru-ru/windows/what-information-event-logs-event-viewer#1TC=windows-7

Все права принадлежат издательству © NOTA BENE (ООО «НБ-Медиа») www.nbpublish.com

DOI: 10.7256/2305-6061.2015.1.14010

При цитировании этой статьи сноска на DOI обязательна