Модель распределения системных событий по приоритетности в автоматизированной системе в защищенном исполнении

И. П. Павлов, email: pavlovvvv1989@gmail.com
А. Б. Сизоненко

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко

Аннотация. *Рассмотрен процесс сбора системных событий в автоматизированной системе в защищенном исполнении, рассмотрены возможные воздействия внешних неблагоприятных факторов на журнал системных событий, предложен способ распределения системных событий на основе их приоритетности, произведено моделирование распределения системных событий по их приоритетности с помощью CPN ML (в сочетании с графическим редактором среды CPN Tools).*

Ключевые слова: *Информационная система, защита информации, автоматизированная система в защищенном исполнении, системные события, внешние факторы.*

Введение

Для предотвращения инцидентов информационной безопасности необходимо проводить анализ огромного количества данных, содержащихся в журналах системных событий. В настоящее время существует большое многообразие представлений журналов системных событий в различных информационных системах. Системные события содержатся в журналах регистрации событий операционных систем серверов и рабочих станций, журналах регистрации событий приложений, журналах регистрации событий средств безопасности, журналах регистрации событий внешнего прокси-сервера, журналах регистрации событий приложений конечного пользователя и в иных источниках.

Защита информации о системных событиях обеспечивается применение мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации и настроек механизмов регистрации

событий. В любой информационной системе подлежат регистрации следующие события [4]:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (установки) операционной системы;
- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

Традиционные средства защиты информации не позволяют обнаружить уже совершенные деструктивные воздействия и оценить ущерб их после реализации, следовательно, нельзя определить меры по предотвращению воздействий внешних факторов на информационную систему [3]. Поэтому важно надежно хранить и анализировать системные события в автоматизированной системе в защищенном исполнении.

1. Процесс сбора системных событий в автоматизированной системе в защищенном исполнении

Напомним, что автоматизированная система в защищенном исполнении – это автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации [1].

В данной статье рассматривается функционирование автоматизированной системы в защищенном исполнении (далее АСЗИ) на семействе операционных систем UNIX. Сбор данных о системных событиях осуществляется средством системного журналирования Syslog. Syslog служит для передачи уведомлений о событиях и использует многоуровневую архитектуру, которая позволяет передавать сообщения на основе разных транспортных протоколов.

Процесс сбора системных событий в АСЗИ изображен на рис. 1, где введены следующие обозначения:

- И1-n – узлы-инициаторы (генерируют содержимое для передачи в сообщениях);

- К1-i – узлы-коллекторы (собирают содержимое сообщений для дальнейшего анализа);

- Т1-m – узлы-трансляторы (пересылают сообщения, принимают сообщения от инициаторов или других трансляторов и передают их коллекторам или другим трансляторам).

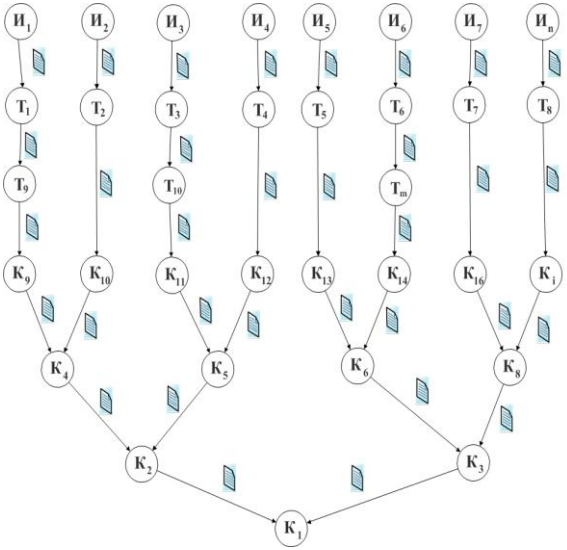

Рис. 1. Процесс сбора системных событий в АСЗИ

2. Возможные неблагоприятные внешние воздействия на журнал системных событий

На журнал с данными о системных событиях, могут воздействовать следующие субъективные внешние факторы [2]:

- доступ к защищаемой информации с применением технических средств;

- несанкционированный доступ к защищаемой информации;

- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

- действия криминальных групп и отдельных преступных субъектов;

- искажение, уничтожение или блокирование информации с применением технических средств.

Специалистами в области защиты информации был выявлен ряд некоторых особенностей, которые в дальнейшем могут привести к

невыполнению заданных функций по регистрации, хранению и анализу информации о системных событиях в конкретной подсистеме, отвечающей за это, а именно [6]:

- отсутствуют механизмы обеспечения целостности передаваемых сообщений, помимо того, что сообщения могут быть отвергнуты, они могут повреждаться при передаче или изменяться злоумышленником, т. е. существует вероятность нарушения целостности сообщения;

- сообщения могут отбрасываться в сети в результате перегрузки, а также перехватываться и отбрасываться с целью сокрытия своих действий, т. е. отсутствует гарантия доставки сообщения;

- отсутствуют механизмы детектирования повторного применения сообщений, злоумышленник может записать набор сообщений, показывающих нормальную работу элемента системы, удалив данный элемент из сети и отправив собранные сообщения транслятору или коллектору, введёт администратора в заблуждение, т. е. существует вероятность повторного использования сообщения.

Проанализировав приведенные данные можно сделать вывод, что существующий способ регистрации и хранения системных событий не позволяет обеспечить выполнение функций по защищенному хранению системных событий, при выходе из строя или уничтожении узлов-коллекторов, собирающих информацию о системных событиях.

3. Распределение системных событий по их приоритетности

Произведенный анализ в пункте 2 данной статьи позволяет выдвинуть гипотезу, заключающаяся в том, что при распределении наиболее важной информации о системных событиях АСЗИ всем узлам коллекторам, мы обеспечим целостность и доступность информации о системных событиях, тем самым обеспечим возможность выполнения функций по регистрации, хранению и анализу системных событий, при возможных неблагоприятных внешних воздействиях на журналы с информацией о системных событиях.

Каждому происходящему событию в Syslog соответствует показатель приоритетности P (Priority), зависящий от двух числовых значений – источника F (Facility) и важности S (Severity). Значения Facility (табл. 1) должны быть в диапазоне от 0 до 23, включительно [6].

Таблица 1

Источники сообщений Syslog

Код	Источник (значимость)
0	Сообщения ядра
1	Сообщения пользовательского уровня
2	Почтовая система

Окончание таблицы 1

Код	Источник (значимость)
3	Системные службы (демоны)
4	Сообщения, связанные с защитой и предоставлением полномочий
5	Внутренние сообщения syslog
6	Подсистема печати (line printer)
7	Подсистема сетевых новостей (network news)
8	Подсистема UUCP
9	Часы (демон)
10	Сообщения, связанные с защитой и предоставлением полномочий
11	Демон FTP
12	Подсистема NTP
13	Аудит (log audit)
14	Сигнал (log alert)
15	Часы (демон)
16	Локальное (local0)
17	Локальное (local1)
18	Локальное (local2)
19	Локальное (local3)
20	Локальное (local4)
21	Локальное (local5)
22	Локальное (local6)
23	Локальное (local7)

Значения Severity (табл. 2) должны быть в диапазоне от 0 до 7, включительно [6].

Таблица 2

Уровни важности сообщений Syslog

Код	Уровень важности
0	Emergency — чрезвычайная ситуация, система не может использоваться
1	Alert — тревога, требуются незамедлительные действия
2	Critical — критическая ситуация
3	Error — ошибка
4	Warning — предупреждение
5	Замечание, нормальная но важная ситуация (состояние)
6	Informational — информационное сообщение
7	Debug — отладочное сообщение

Показатель приоритетности P рассчитывается по формуле (1) [6].

$$P = 8 \cdot F + S \quad (1)$$

Соответственно, чем значение P меньше, тем приоритетность сообщения выше.

С помощью CPN ML (в сочетании с графическим редактором среды CPN Tools) произведем моделирование алгоритма распределения системных событий по приоритетности на рис.2.

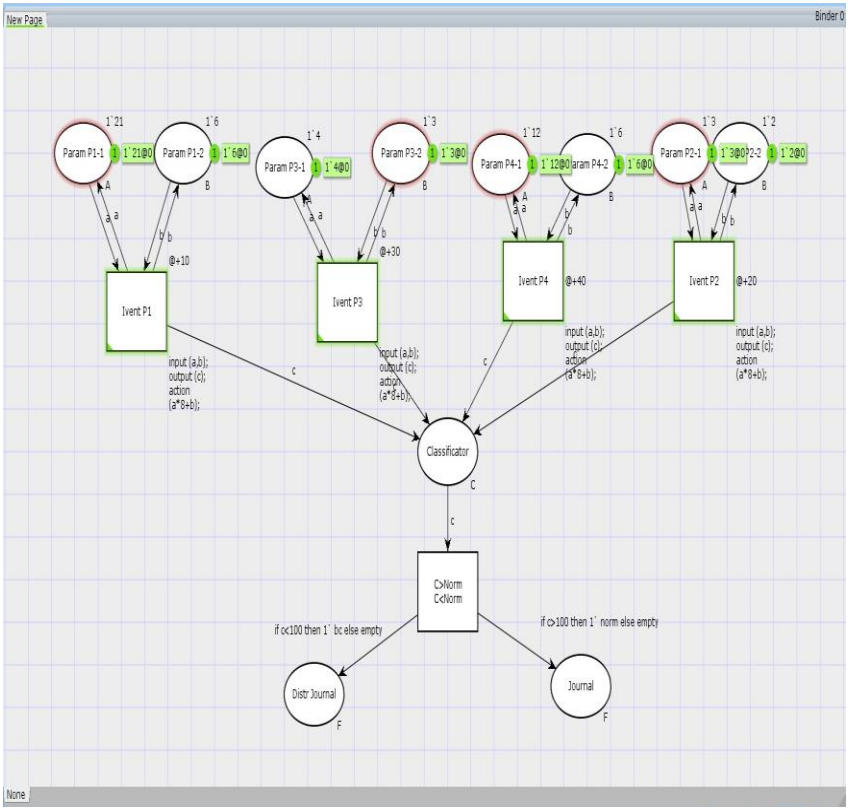

Рис. 2. Графическое представление работы программы

На данном рисунке системным событиям (их 4) соответствуют переходы Ivent P1, Ivent P2, Ivent P3, Ivent P4. У Каждого соответствующего системного события есть значения Facility, которому соответствуют позиции Param P1-1, Param P2-1, Param P3-1, Param P4-1 и есть значения Severity, которым соответствуют позиции Param P1-2,

Param P2-2, Param P3-2, Param P4-2. Значения Facility и Severity задаются значениями из таблиц 1,2. Далее в позицию Classificator поступают вычисленные значения показателя приоритетности системного события P по формуле (1). После этого полученные значения P поступают в переход, который выполняет функцию фильтра, в данном случае пороговое значение P=100. В итоге алгоритм работы программы заканчивается распределением четырех системных событий с заданными значениями Facility и Severity по журналам регистрации системных событий, которым соответствуют позиции Distr Journal и Journal.

Используя данный алгоритм, мы распределим системные события по их приоритетности на два журнала, в одном будет храниться наиболее важная информация, а во втором журнале будут находиться все остальные системные события. Распределение информации о системных событиях позволит сэкономить время для анализа огромной информации о системных событиях в автоматизированной системе в защищенном исполнении, так как анализу будут подвергнута только важная информация о системных событиях.

4. Формат записи информации о системном событии, вносимый в распределенный реестр

При воздействии внешних неблагоприятных факторов на журналы системных событий в АСЗИ, может сложиться ситуация, когда журнал системных событий может быть изменен или уничтожен, а это в свою очередь не позволит произвести мониторинг событий, и мы не сможем выяснить причин, повлекших за собой серьёзные последствия для безопасности АСЗИ.

Для обеспечения целостности и защиты от модификации наиболее важной информации о системных событиях предлагается использовать распределенный реестр [5].

Предлагается формат записи информации о системном событии в поле SCI (stored control information), изображенного на рис. 3.

Поля DATA, TS, ID, IDP, IS, IN формируются автоматически при регистрации события. Помимо самого события его хэш-код (HD) также вносится в регистрационную запись. Это является дополнительной мерой защиты целостности информации о системном событии и практически исключит возможность несанкционированного внесения в неё изменений. Запись подписывается ключом подписи пользователя (конкретного узла-коллектора или узла-транслятора).

Далее заполненные поля SCI группируются в блоки и заносятся в распределенный реестр [5].

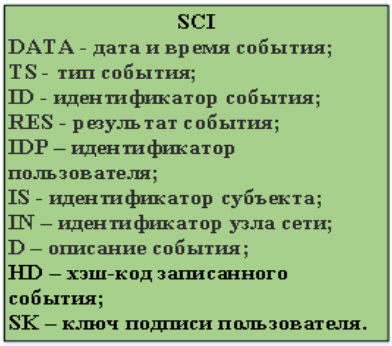

Рис. 3. Формат записи информации о системном событии

Заключение

Предложенный способ распределения и регистрации системных событий позволит уменьшить время, затрачиваемое на их анализ, обеспечит целостность и доступность информации при воздействиях субъективных внешних факторов, а также обеспечит защиту журналов системных событий АСЗИ от модификации.

Список литературы

1. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения : ГОСТ Р 51583-2014 – Введ. 01.09.2014. – М. : Стандартинформ, 2014. - 21с.

2. Защита информации. Объект информатизации. Факторы, воздействующие на информацию : ГОСТ Р 51275-2006 – Введ. 27.12.2006. – М. : Стандартинформ, 2006. - 12с.

3. Лукацкий, А. В. Обнаружение атак : / А. В. Лукацкий : БХВ-Петербург, 2001. – 563 с.

4. Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/675

5. Павлов, И.П. Способ распределения информации журналов событий информационной безопасности в корпоративной информационной системе на основе технологии Блокчейн / И.П. Павлов, А.Б. Сизоненко // «Российская наука в современном мире» XXXII Международная научно-практическая конференция. – 2020. – С. 50-53.

6. Энциклопедия сетевых протоколов: Протокол Syslog [Электронный ресурс]. – Режим доступа: https://www.protocols.ru/WP/wp-content/uploads/2017/10/rfc5424.pdf