**XX Международная конференция**
**«Информатика: проблемы, методы, технологии» (IPMT-2020)**

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

**Докладывает: адъюнкт Павлов И.П.**
**Научный руководитель: д.т.н., доцент Сизоненко А.Б.**

# НОРМАТИВНО-ПРАВОВАЯ БАЗА, РЕГЛАМЕНТИРУЮЩАЯ ТРЕБОВАНИЯ К СИСТЕМНЫМ СОБЫТИЯМ



ГОСТ Р 54471-2011/ISO/TR 15801:2009 СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА УПРАВЛЕНИЕ ДОКУМЕНТАЦИЕЙ. ИНФОРМАЦИЯ, СОХРАНЯЕМАЯ В ЭЛЕКТРОННОМ ВИДЕ. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ДОСТОВЕРНОСТИ И НАДЕЖНОСТИ (п. 7.1.4, 7.1.6)

МЕТОДИЧЕСКИЙ ДОКУМЕНТ: «МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ», УТВЕРЖДЕН ФСТЭК РОССИИ 11 ФЕВРАЛЯ 2014 ГОДА (п. 3.5.1)

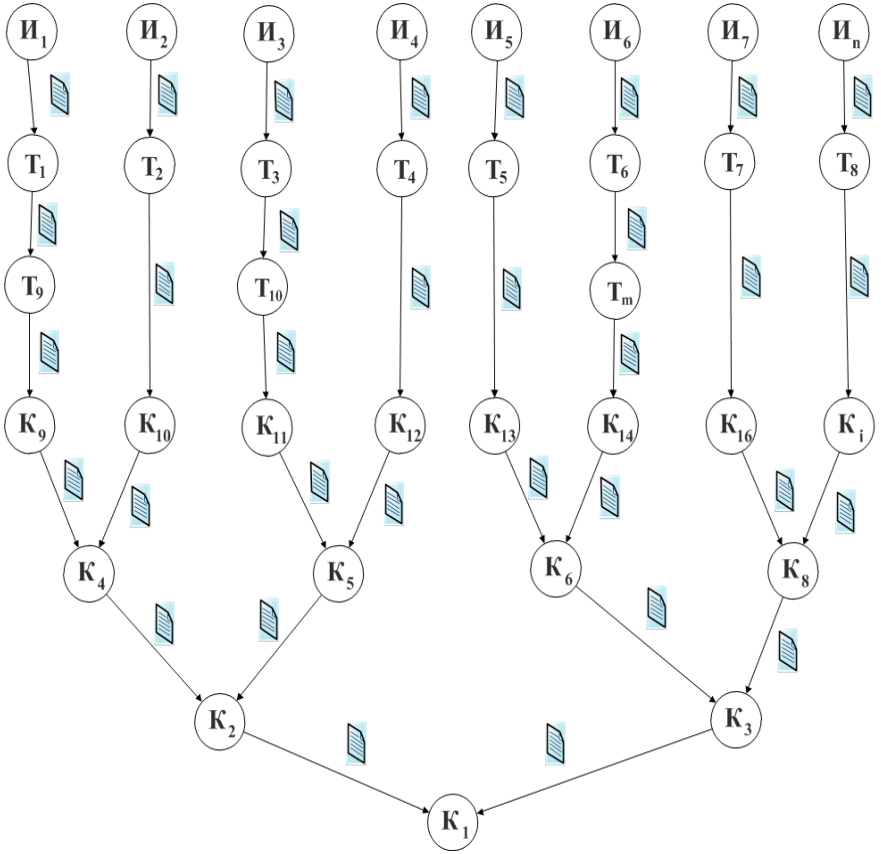
ГОСТ Р 51583-2014 ЗАЩИТА ИНФОРМАИИ. ПОРЯДОК СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ. ОБЩИЕ ПОЛОЖЕНИЯ: (п. 5.2)

ГОСТ Р ИСО/МЭК 15408-2-2013 ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ (ИТ). МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. ЧАСТЬ 2. ФУНКЦИОНАЛЬНЫЕ КОМПОНЕНТЫ БЕЗОПАСНОСТИ (п. 7.2.2)

В АС должна обеспечиваться защита информации, связанной с действиями, относящимися к безопасности. Защита информации обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации и настроек механизмов регистрации событий. Традиционные средства защиты информации не позволяют обнаружить уже совершенные деструктивные воздействия и оценить ущерб их после реализации и следовательно, нельзя определить меры по предотвращению воздействия внешних факторов.

# ПРОЦЕСС СБОРА СИСТЕМНЫХ СОБЫТИЙ В АСЗИ






ПРИМЕНЯЕМЫЕ ОБОЗНАЧЕНИЯ

**И**$_{1-n}$ – узлы инициаторы (генерируют содержимое для передачи в сообщениях syslog);

**К**$_{1-i}$ – узлы коллекторы (собирают содержимое сообщений syslog для дальнейшего анализа);

**Т**$_{1-m}$ – узлы трансляторы (пересылают сообщения, принимают сообщения от инициаторов или других трансляторов и передают их коллекторам или другим трансляторам).

# ФАКТОРЫ ВОЗДЕЙСТВУЮЩИЕ НА ПОДСИСТЕМУ ХРАНЕНИЯ СИСТЕМНЫХ СОБЫТИЙ АС



| ОБЪЕКТИВНЫЕ ФАКТОРЫ | | СУБЪЕКТИВНЫЕ ФАКТОРЫ | |
|---|---|---|---|
| **Внутренние факторы** | **Внешние факторы** | **Внутренние факторы** | **Внешние факторы** |
| Передача сигналов | Явления техногенного характера | Разглашение защищаемой информации лицами, имеющими к ней право доступа | Доступ к защищаемой информации с применением технических средств |
| Излучения сигналов, функционально присущие техническим средствам | Природные явления, стихийные бедствия | Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации | Несанкционированный доступ к защищаемой информации |
| Побочные электромагнитные излучения | | Несанкционированный доступ к информации | Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку |
| Паразитное электромагнитное излучение | | Недостатки организационного обеспечения защиты информации | Действия криминальных групп и отдельных преступных субъектов |
| Наводка | | Ошибки обслуживающего персонала | Искажение, уничтожение или блокирование информации с применением технических средств |
| Наличие акустоэлектрических преобразователей в элементах технических средств | | | |
| Дефекты, сбои и отказы, аварии | | | |
| Дефекты, сбои и отказы программного обеспечения | | | |

1. Отсутствуют механизмы обеспечения целостности передаваемых сообщений. Помимо того, что сообщения могут быть отвергнуты, они могут повреждаться при передаче или изменяться злоумышленником. Существует вероятность нарушения целостности сообщения.

2. Сообщения могут отбрасываться в сети в результате перегрузки, а также перехватываться и отбрасываться с целью сокрытия своих действий. Отсутствует гарантия доставки сообщения.

3. 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. Существует вероятность повторного использования сообщения.

# РАСПРЕДЕЛЕНИЕ СИСТЕМНЫХ СОБЫТИЙ ПО ИХ ПРИОРИТЕТНОСТИ

**Показатель приоритетности P рассчитывается по следующей формуле:**

$$P=8*F+S$$

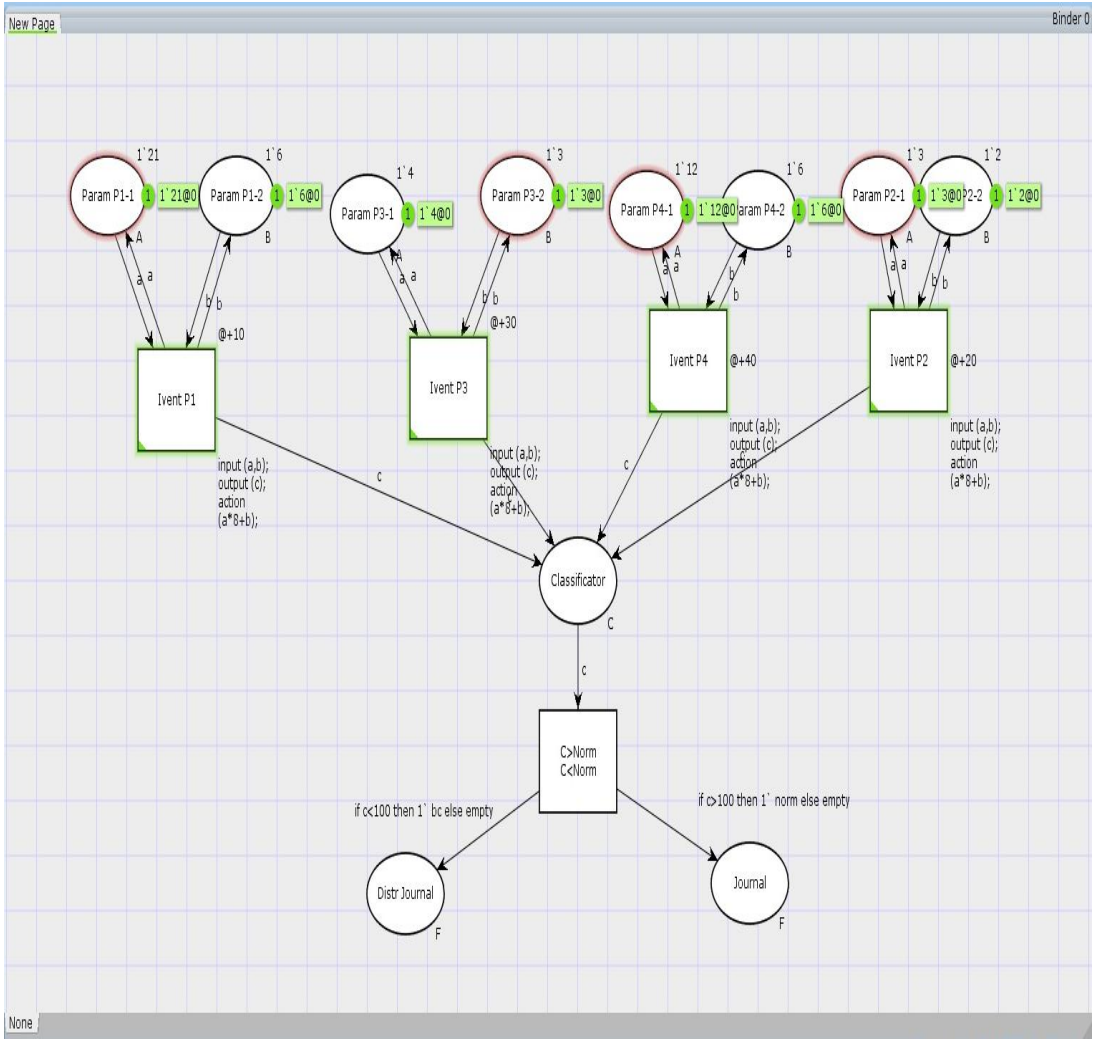
**Соответственно, чем значение P меньше, тем приоритетность сообщения выше.**

**Используя приоритетность системных событий произведем распределение сообщений от периферийных устройств в АСЗИ.**

**С помощью CPN ML (в сочетании с графическим редактором среды CPN Tools) произведем моделирование алгоритма распределения системных событий по приоритетности, алгоритм основан на вычислении показателя приоритетности P, исходя из соответствующих исходных значений системных событий Facility и Severity в протоколе Syslog.**

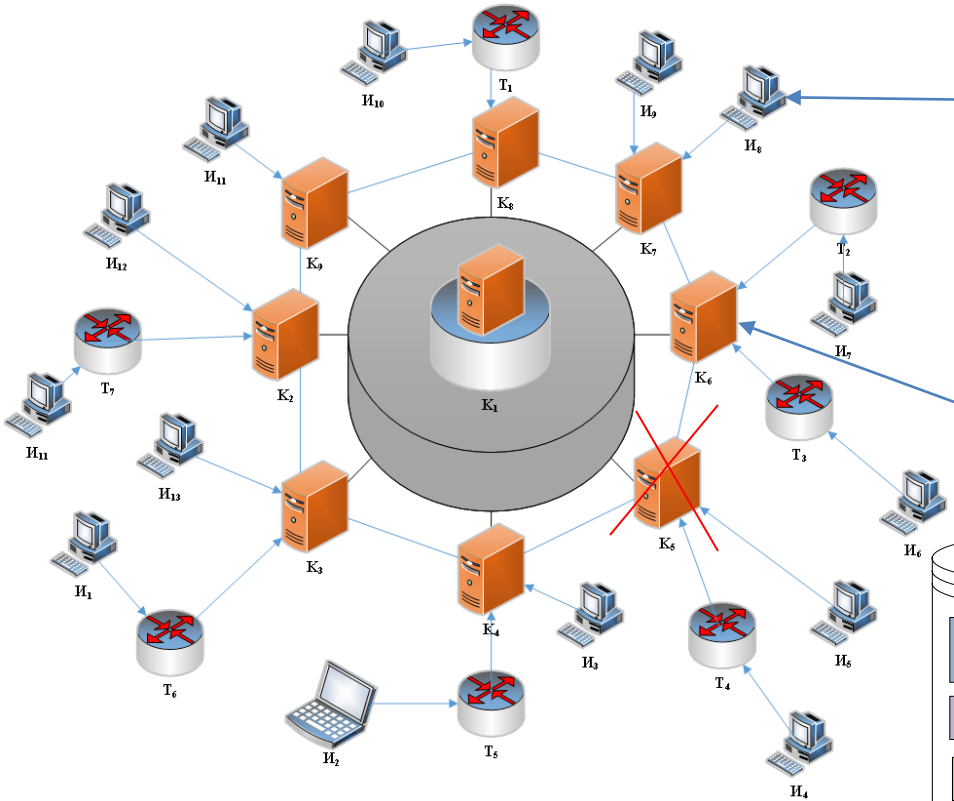
# ГРАФИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ РАБОТЫ ПРОГРАММЫ





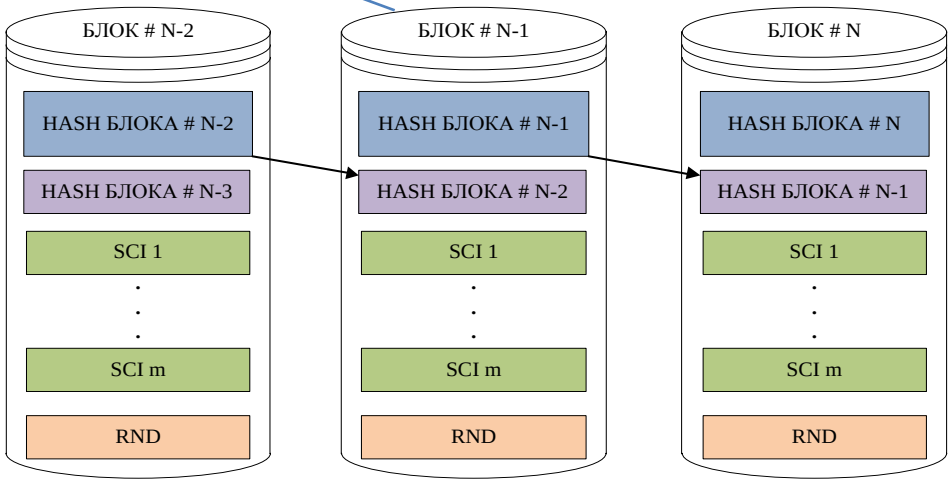
# МОДЕЛЬ ПОДСИСТЕМЫ ХРАНЕНИЯ СИСТЕМНЫХ СОБЫТИЙ АСЗИ НА ОСНОВЕ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ






**SCI**

DATA - дата и время события;
TS - тип события;
ID - идентификатор события;
RES - результат события;
IDP – идентификатор пользователя;
IS - идентификатор субъекта;
IN – идентификатор узла сети;
D – описание события;
HD – хэш-код записанного события;
SK – ключ подписи пользователя.



**СПАСИБО ЗА ВНИМАНИЕ !**