105318 г. Москва, ул. Ибрагимова, д. 31
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

РУССКО-АНГЛИЙСКИЙ ГЛОССАРИЙ ПО ТЕМЕ УПРАВЛЕНИЯ СОБЫТИЯМИ

Источник определения	Определение
Событие (Event)	
NIST	Something that occurs within a system or network
NIST (перевод)	Что-то, что происходит в системе или сети
ITIL	A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item or monitoring tool. Events typically require IT operations personnel to take actions, and often lead to incidents being logged
ITIL (перевод)	Изменение состояния, которое имеет значение для управления ИТ-услугой или другой конфигурационной единицей. Этот термин также используется для обозначения оповещения или уведомления, созданного любой ИТ-услугой, конфигурационной единицей или средством мониторинга. События обычно требуют от персонала эксплуатации ИТ выполнения действий, и часто приводят к регистрации инцидентов
Инцидент (Incident)	
ITIL	Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service
ITIL (перевод)	Незапланированное прерывание или снижение качества ИТ-услуги
Комментарий	Сбой конфигурационной единицы, который еще не повлиял на ИТ-услугу, также является инцидентом, как, например, сбой одного диска из массива зеркалирования
Агрегация событий (Event Aggregation)	
NIST	The consolidation of similar log entries into a single entry containing a count of the number of occurrences of the event
NIST (перевод)	Объединение схожих записей в лог-журнале в одну запись, содержащую количество произошедших событий (о которых сообщается в данных записях)

Источник определения	Определение
Корреляция событий (Event Correlation)	
NIST	Finding relationships between two or more log entries
NIST (перевод)	Поиск взаимосвязей между двумя или более записями в лог-журналах
Комментарий	Поиск взаимосвязей между событиями и определение значения (смысла) такой взаимосвязи
Фильтрация событий (Event Filtering)	
NIST	The suppression of log entries from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest
NIST (перевод)	Исключение записей лог-журналов из анализа, отчетов или долговременного хранения, основываясь на определенных параметрах данных записей, характеризующих, что, скорее всего, они не содержат информацию, представляющую какой-либо интерес
Редукция событий (Event Reduction)	
NIST	Removing unneeded entries from a log to create a new log that is smaller
NIST (перевод)	Удаление записей, не несущих полезной информации, из лог-журналов для создания нового лог-журнала меньшего размера
Управление событиями (Log management)	
NIST	The process for generating, transmitting, storing, analyzing, and disposing of log data
NIST (перевод)	Процесс, обеспечивающий генерацию, передачу, хранение, анализ и распределение/ликвидацию сообщений о событиях

105318 г. Москва, ул. Ибрагимова, д. 31
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru

Источник определения	Определение
Инфраструктура управления событиями (Log Management Infrastructure)	
NIST	The hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data
NIST (перевод)	Аппаратное и программное обеспечение, сети и медиа, используемые для генерации, передачи, хранения, анализа и распределения / ликвидации сообщений о событиях
Нормализация сообщений о событиях (Log Normalization)	
NIST	Converting each log data field to a particular data representation and categorizing it consistently
NIST (перевод)	Конвертация каждого поля сообщения о событии в подходящее представление данных и соответствующая категоризация
Комментарий	Имеется ввиду, категоризация конкретного поля, например: User=Username=Пользователь
Разбор / парсинг сообщений о событиях (Log Parsing)	
NIST	Extracting data from a log so that the parsed values can be used as input for another logging process
NIST (перевод)	Выделение данных из сообщения о событии таким образом, чтобы выделенные значения могли использоваться как входные данные для другого процесса работы с сообщениями о событии
Обеспечение сохранности сообщений о событиях (Log Preservation)	
NIST	Keeping logs that normally would be discarded, because they contain records of activity of particular interest
NIST (перевод)	Обеспечение сохранности сообщений о событиях, которые обычно удаляются, но в частном случае содержат записи об активностях, представляющих интерес

Источник определения	Определение
Редукция логов (Log Reduction)	
NIST	Removing unneeded entries from a log to create a new log that is smaller
NIST (перевод)	Удаление ненужных записей из лога для создания нового лога меньшего размера
Отчетность о событиях (Log Reporting)	
NIST	Displaying the results of log analysis
NIST (перевод)	Отображение результатов анализа сообщений о событиях
Хранение сообщений о событиях (Log Retention)	
NIST	Archiving logs on a regular basis as part of standard operational activities
NIST (перевод)	Архивирование сообщений о событиях на регулярной основе как часть стандартных процедур
Ротация файлов журналов событий (Log Rotation)	
NIST	Closing a log file and opening a new log file when the first log file is considered to be complete
NIST (перевод)	Закрытие файла журнала события и открытие нового файла, когда первый файл определен как завершенный
Корреляция событий на основе правил (Rule-Based Event Correlation)	
NIST	Correlating events by matching multiple log entries from a single source or multiple sources based on logged values, such as timestamps, IP addresses, and event types
NIST (перевод)	Корреляция событий путем сопоставления множества записей сообщений о событиях из одного или различных источников на основе значений сообщений, таких как временные метки, IP-адреса и типы событий

В Глоссарии приведены (переведены) определения из следующих документов:

- **NIST** – National Institute of standards and technology. Special Publication 800-92. Guide to Computer Security Log Management;
- **ITIL** – IT Infrastructure Library. Glossary.