Вопросы доступности информации от различных источников событий

Александр Кузнецов, CISM, MVP

Руководитель направления ИБ ООО «НТЦ «Вулкан»

Аспирант кафедры «ИБ» Финансового университета при Правительстве РФ

21.11.2017

www.ntc-vulkan.ru

СОДЕРЖАНИЕ

Источники событий

Источник событий – это программное, программно-аппаратное решение или сервис, поставляющий информацию об изменении или сохранении состояния, которое имеет значение для безопасности, управления и/или работоспособности системы

К источникам событий относятся:

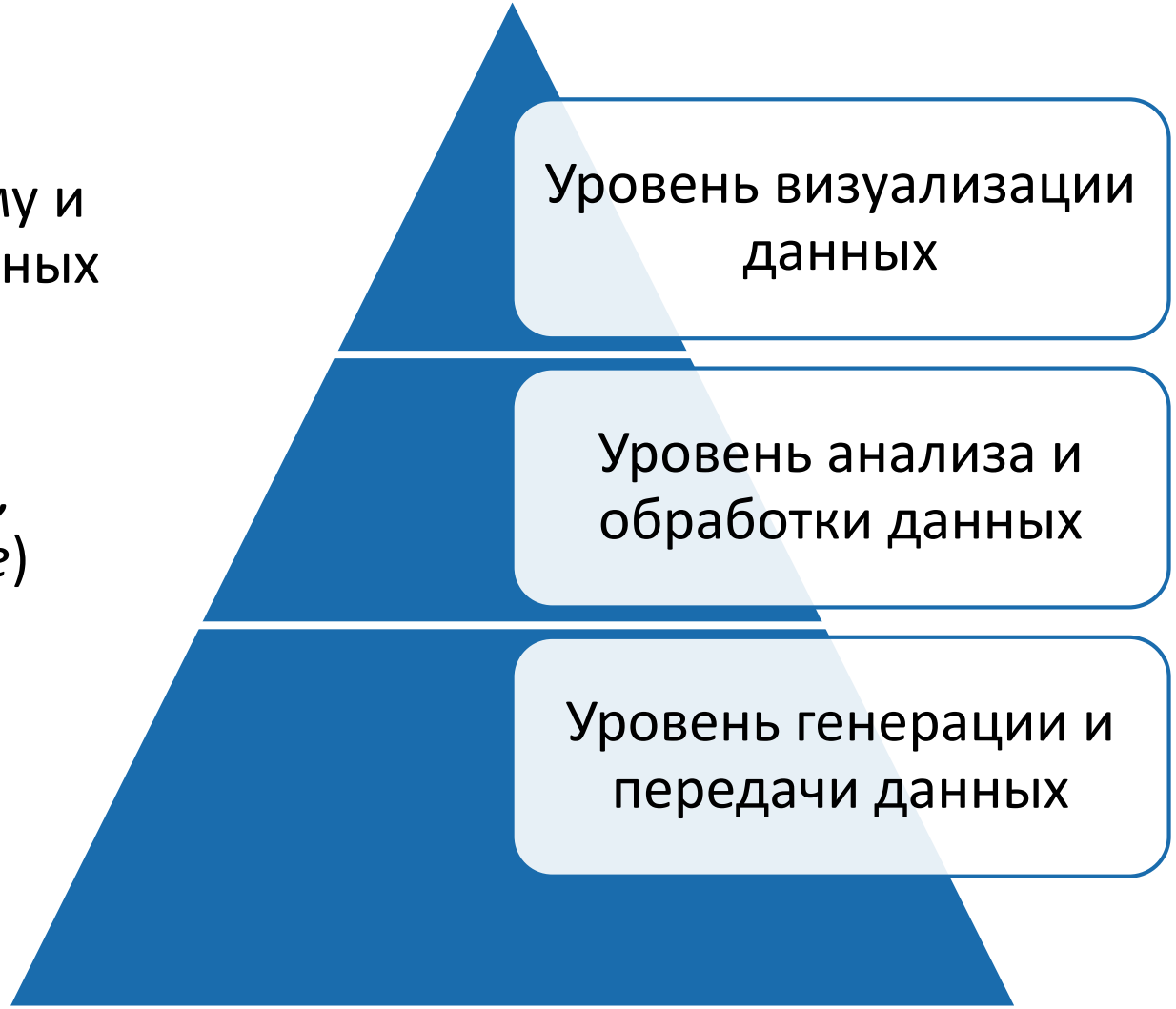
- СрЗИ (*САЗ, МЭ, СОВ и т.п.*), СКЗИ, средства контроля и анализа защищенности
- Системное ПО (*ОС, гипервизоры и т.п.*)
- Прикладное ПО (*СУБД, веб-приложения и т.п.*)
- Поставщики сетевых пакетов (*АСО через SPAN-порт, TAP-устройства и т.п.*)

Источники событий условно делятся на:

- *pull* – нужно забрать информацию
- *push* – сам отдает информацию

Роль и место источников событий в ЦМИБ организации

- Выполнение задач по своевременному и информативному представлению данных
- Выполнение аналитических задач (*агрегация, обогащение др. данными, корреляция данных, прогнозирование*)
- Выполнение целевых задач
- Регистрация событий по факту выполнения целевых задач



Условия для доступности информации

Необходимые условия

- Возможность зарегистрировать информацию
- Возможность предоставить доступ к зарегистрированной информации

Условия для доступности информации

Необходимые условия

- Возможность зарегистрировать информацию
- Возможность предоставить доступ к зарегистрированной информации

«Достаточные условия»

- Читаемость информации

	CG_NAME	SL_CATEGORY	SL_TIMEGENERATED	SL_DATASHORT
1	ЦУС	40	2016-02-12 07:10:13.000	0x540000000100000000000000000000000020000080D0C028...
2	ЦУС	40	2016-02-12 07:38:56.000	0x5E0000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E...
3	КШ с ЦУСом	35	2016-02-12 07:40:35.000	0x6D000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2...
4	ЦУС	40	2016-02-12 07:42:55.000	0x540000000100000000000000000000000020000090E0C028...
5	КШ с ЦУСом	40	2016-02-12 07:42:13.000	0x540000000100000000000000000000000525649534F52000000...
6	ЦУС	35	2016-02-12 07:45:27.000	0xD0000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2...
7	ЦУС	40	2016-02-12 07:58:00.000	0x5F0000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E...
8	ЦУС	40	2016-02-12 08:15:26.000	0x5E0000000000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8E...
9	КШ с ЦУСом	35	2016-02-12 08:19:08.000	0x74000000C2F1F2F0EEE5EDEDFBE920E0E4ECE8EDE8F1F2F...

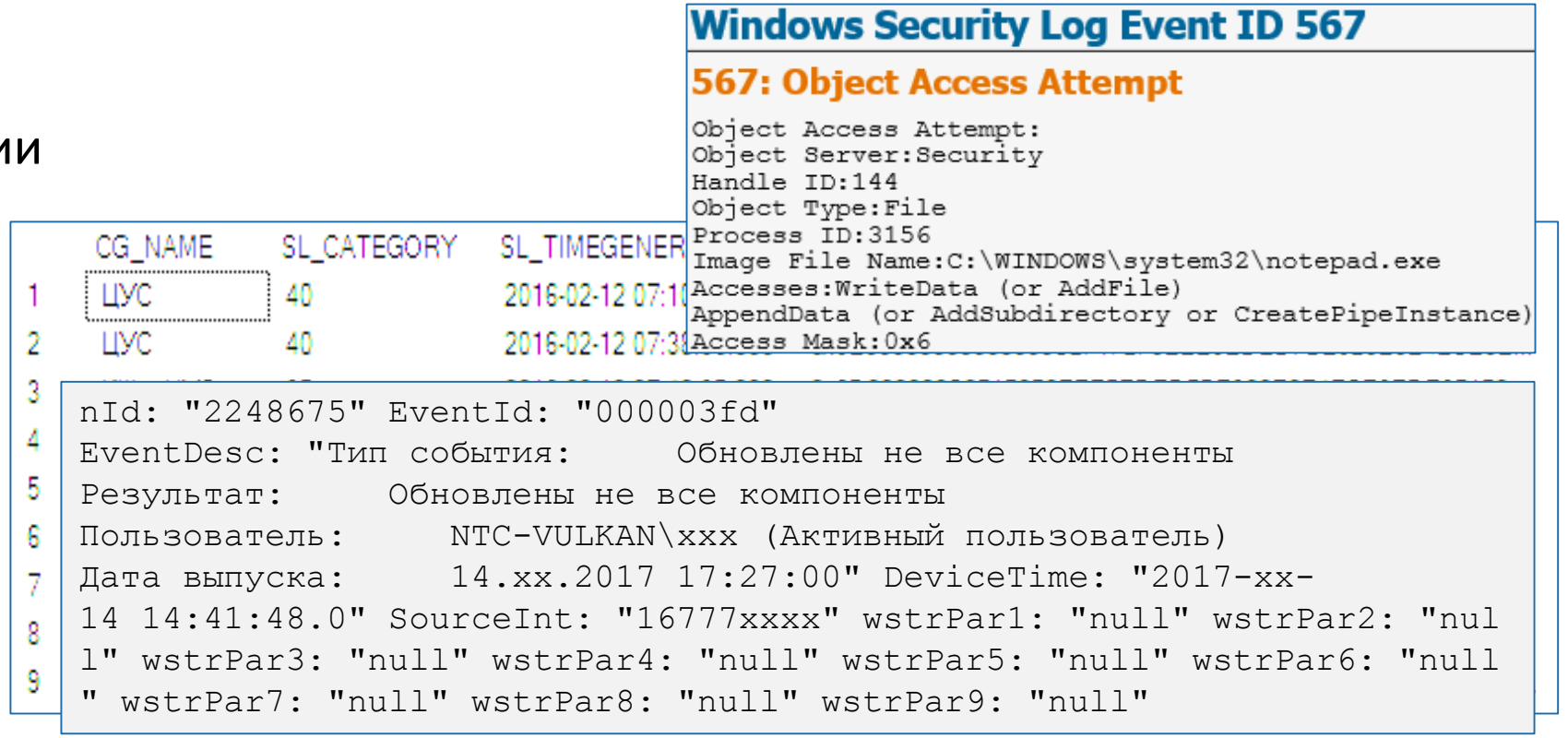
Условия для доступности информации

Необходимые условия

- Возможность зарегистрировать нужную вам информацию
- Возможность предоставить доступ к зарегистрированной информации

«Достаточные условия»

- Читаемость информации
- Наличие необходимых данных



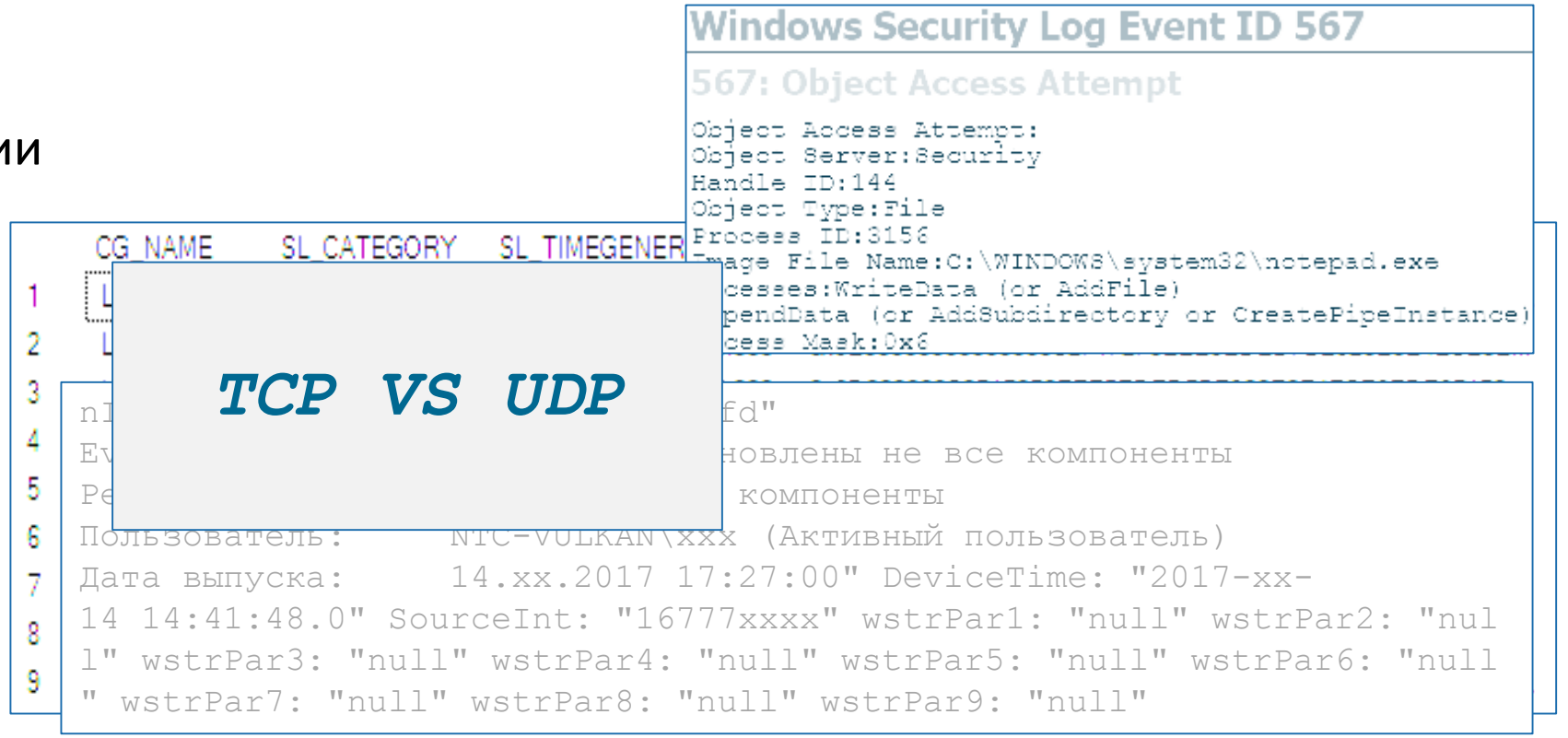
Условия для доступности информации

Необходимые условия

- Возможность зарегистрировать нужную вам информацию
- Возможность предоставить доступ к зарегистрированной информации

«Достаточные условия»

- Читаемость информации
- Наличие необходимых данных
- Гарантированная доставка информации



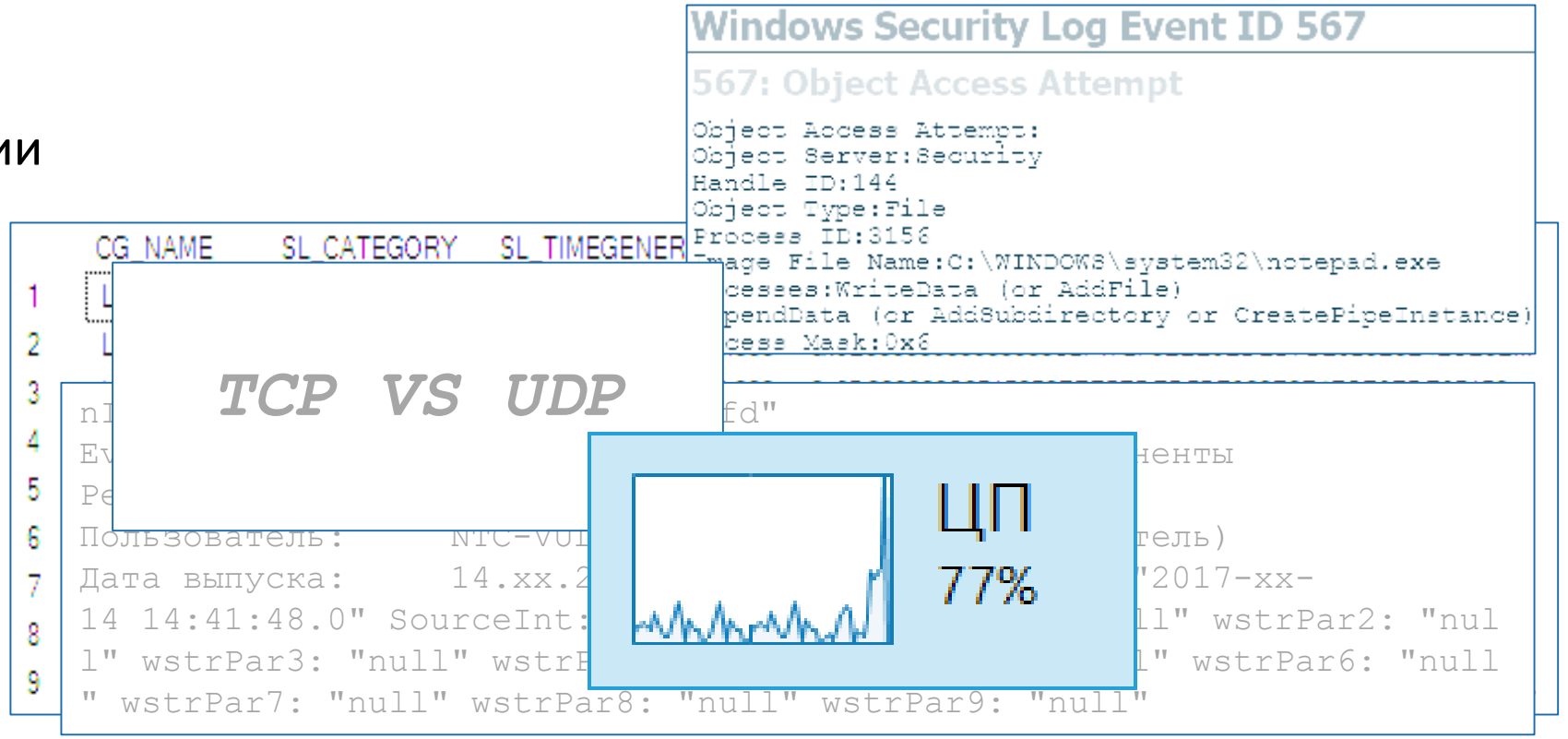
Условия для доступности информации

Необходимые условия

- Возможность зарегистрировать нужную вам информацию
- Возможность предоставить доступ к зарегистрированной информации

«Достаточные условия»

- Читаемость информации
- Наличие необходимых данных
- Гарантированная доставка информации
- Наличие мощностей у источника событий



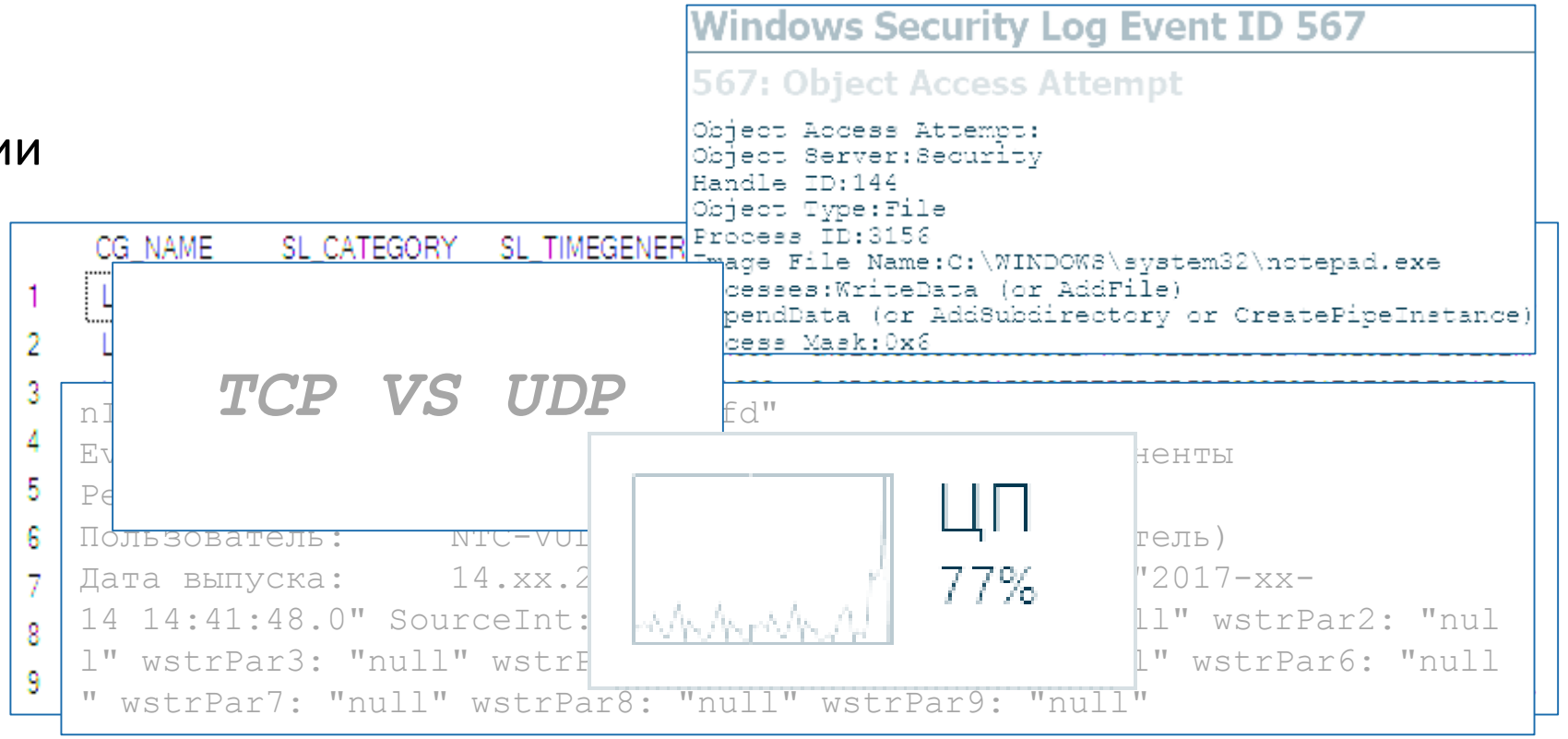
Условия для доступности информации

Необходимые условия

- Возможность зарегистрировать нужную вам информацию
- Возможность предоставить доступ к зарегистрированной информации

«Достаточные условия»

- Читаемость информации
- Наличие необходимых данных
- Гарантированная доставка информации
- Наличие мощностей у источника событий
- Корректный приём системой мониторинга



Стандартизация форматов данных

<190>%ASA-6-113008: AAA transaction status ACCEPT : user = x.xxx

<190>%ASA-6-113009: AAA retrieved default group policy (NOACCESS) for user = x.xxx

<190>%ASA-6-113004: AAA user authentication Successful : server = 10.0.0.22 : user = x.xxx

nId: "2245895" EventId: "KLAUD_EV_SERVERCONNECT" EventDesc: "Пользователь "NTC-VULKAN\x.xxx" подключился к Серверу администрирования с адреса “x.x.x.x"" DeviceTime: "2017-xx-xx 09:06:59.0“ SourceInt: "213070xxxx“ wstrPar1: "null“ wstrPar2: “x.x.x.x“ wstrPar3: "NTC-VULKAN\x.xxx“ wstrPar4: "null" wstrPar5: “x.x.x.x“ wstrPar6: "null" wstrPar7: "null“ wstrPar8: "null“ wstrPar9: "null"

SourceIp=x.x.x.x AgentDevice=WindowsExchange AgentLogFile=RECV2017xxxx-1.LOG AgentLogFormat=SMTP date-time=2017-xx-xxT14:59:48.657Z connector-id=xxxx\Default Frontend xxxx session-id=08D516554065B80F sequence-number=10 local-endpoint=x.x.x.x:25 remote-endpoint=x.x.x.x:xxx event=> data=250-STARTTLS context=

Стандартизация форматов данных

Состав события (*ИСО/МЭК 15408*):

- дата и время события
- тип события
- идентификатор субъекта
- результат события (*успешный или неуспешный*)

Состав события (*Меры ЗИ в ГИС*):

- тип события
- дата и время события
- идентификационная информация источника события
- результат события (*успешный или неуспешный*)
- субъект доступа, связанные с данным событием

Syslog: 40 полей (*Request for Comments: 5424*)

Формат данных: Дата и время

Nov 21 2017 11:16:56 GMT

Nov 21, 2017, 2:16:56 PM

2017-11-21 14:16:56.384

2017-11-21T14:16:56.384Z

2017-11-21 14:16:56+0200

2017/11/21 14:16:56

21.11.2017 14:16:56

2017-11-21 14:16:56

1510918738

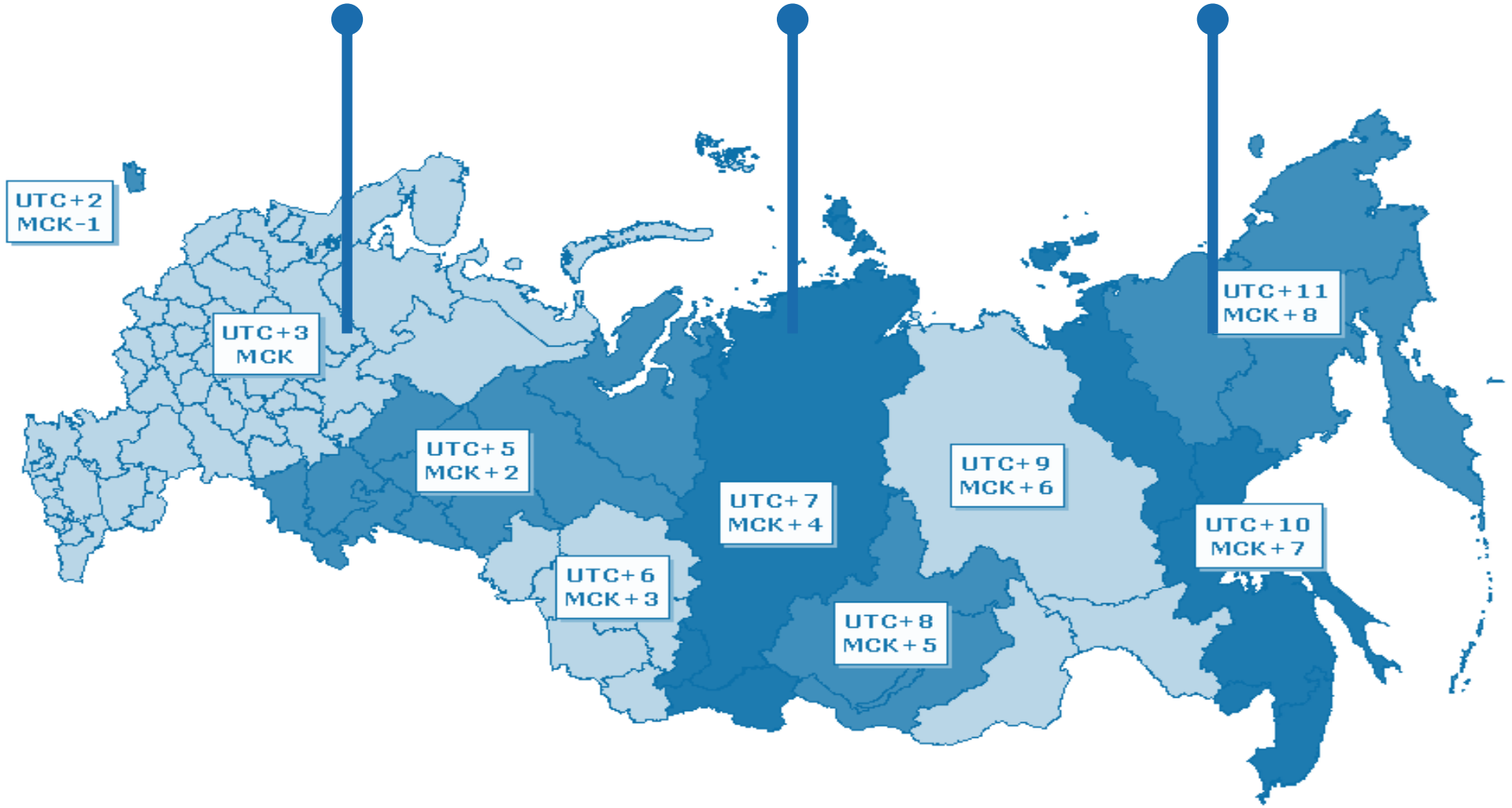
Nov 21 14:16:56

```
FULL-TIME       = PARTIAL-TIME TIME-OFFSET
PARTIAL-TIME    = TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND
                  [TIME-SECFRAC]
TIME-HOUR       = 2DIGIT  ; 00-23
TIME-MINUTE     = 2DIGIT  ; 00-59
TIME-SECOND     = 2DIGIT  ; 00-59
TIME-SECFRAC    = "." 1*6DIGIT
TIME-OFFSET     = "Z" / TIME-NUMOFFSET
TIME-NUMOFFSET  = ("+" / "-") TIME-HOUR ":" TIME-MINUTE
```

```
TIMESTAMP       = NILVALUE / FULL-DATE "T" FULL-TIME
FULL-DATE       = DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY
DATE-FULLYEAR   = 4DIGIT
DATE-MONTH      = 2DIGIT  ; 01-12
DATE-MDAY       = 2DIGIT  ; 01-28, 01-29, 01-30, 01-31 based on
                          ; month/year
```

Формат данных: Дата и время: Учёт часовых поясов

Δt между событиями: 0 мин. +1 мин. +2 мин.



Формат данных: Дата и время: Учёт часовых поясов

Δt между событиями: 0 мин. +1 мин. +2 мин.

Время событий: 16:00 20:01 00:02

Формат данных: Дата и время: Учёт часовых поясов

Δt между событиями: 0 мин. +1 мин. +2 мин.

Время событий: 16:00 20:01 00:02

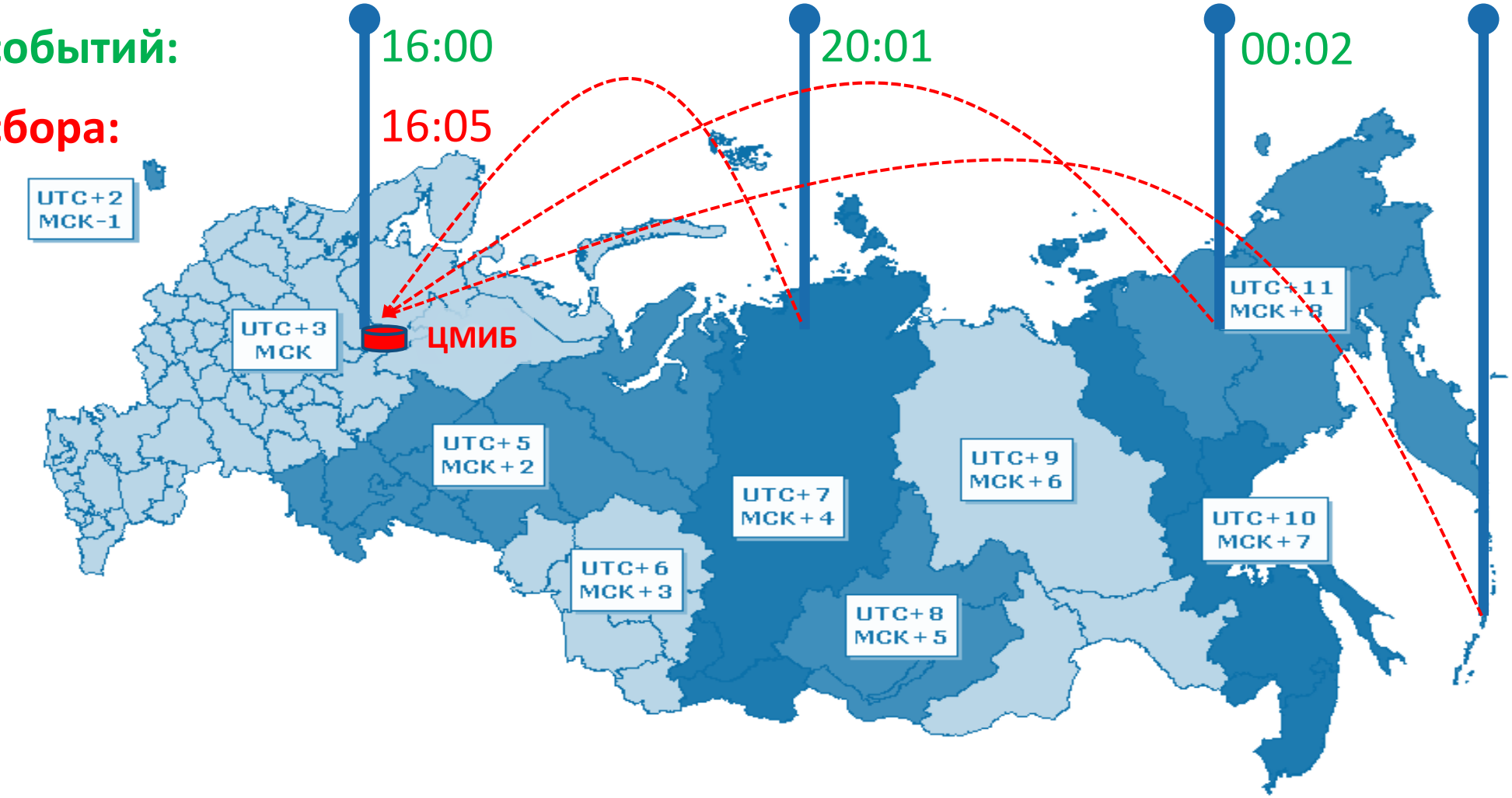
Время сбора: 16:05

Формат данных: Дата и время: Учёт часовых поясов

Δt между событиями: 0 мин. +1 мин. +2 мин.

Время событий: 16:00 20:01 00:02

Время сбора: 16:05



Пачка событий

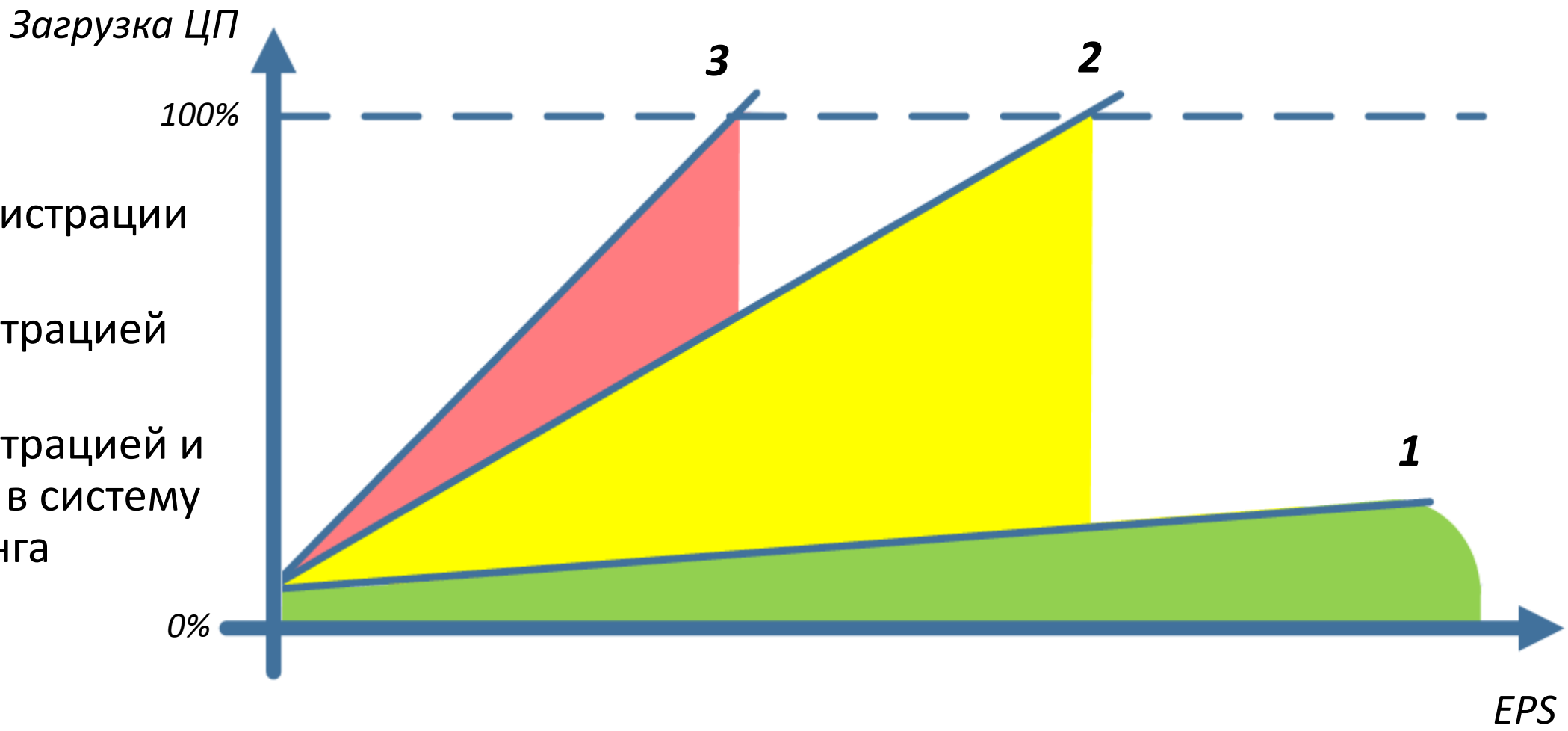
00:01
00:02
...
23:58
23:59

Нагрузка на источник событий

1 – Без регистрации событий

2 – С регистрацией событий

3 – С регистрацией и отправкой в систему мониторинга



Корректный приём информации

«Зона ответственности» системы мониторинга:

- Корректная фильтрация событий – не отбросить нужное
- Корректный парсинг событий – выделить нужное
- Обработка пиковых потоков событий – не потерять нужное

Заключение

- Источники событий – это основа любого ЦМИБ организации
- Наличие источника событий ≠ наличие необходимой информации
- Добивайтесь доступности необходимой информации (*настройкой или доработкой*)
- Ищите баланс между «глубиной» аудита и производительностью источника событий
- Участвуйте в решении вопроса стандартизации функции аудита событий

СПАСИБО ЗА ВНИМАНИЕ!

Александр Кузнецов

Руководитель направления ИБ

+7 (495) 777-13-10

a.kuznetsov@ntc-vulkan.ru

www.ntc-vulkan.ru