

|   | РАЗОВЫЙ<br>МОНИТОРИНГ | ОПЕРАТИВНЫЙ<br>МОНИТОРИНГ | ОПЕРАТИВНЫЙ<br>МОНИТОРИНГ | УПРАВЛЕНИЕ<br>ИНЦИДЕНТАМИ | УПРАВЛЕНИЕ<br>ИНЦИДЕНТАМИ |
|---|-----------------------|---------------------------|---------------------------|---------------------------|---------------------------|
| <b>В БАЗОВЫЙ КОМПЛЕКТ ВКЛЮЧЕНЫ</b>                      |                       | <b>9x5</b>                | <b>24x7</b>               | <b>9x5</b>                | <b>24x7</b>               |
| Компонент NIDS, HIDS                                    | +                     | +                         | +                         | +                         | +                         |
| Компонент CMDB  | +                     | +                         | +                         | +                         | +                         |
| Визуализация (web-консоли)                              | +                     | +                         | +                         | +                         | +                         |
| Стандартные типы источников                             | <b>&gt;50</b>         | <b>&gt;50</b>             | <b>&gt;50</b>             | <b>&gt;50</b>             | <b>&gt;50</b>             |
| Стандартные правила корреляции                          |                       | <b>&gt;300</b>            | <b>&gt;300</b>            | <b>&gt;300</b>            | <b>&gt;300</b>            |
| <b>ПАРАМЕТРЫ УСЛУГИ (SLA)</b>                           |                       |                           |                           |                           |                           |
| Количество событий в секунду*                           | ∞                     | ∞                         | ∞                         | ∞                         | ∞                         |
| Гарантированный уровень доступности услуги              | <b>99%</b>            | <b>99%</b>                | <b>99%</b>                | <b>99%</b>                | <b>99%</b>                |
| Сбор/прием/хранение/обработка событий ИБ                | <b>24x7</b>           | <b>24x7</b>               | <b>24x7</b>               | <b>24x7</b>               | <b>24x7</b>               |
| Мониторинг и анализ событий, выявление инцидентов       |                       | <b>9x5</b>                | <b>24x7</b>               | <b>9x5</b>                | <b>24x7</b>               |
| Мониторинг работоспособности                            | <b>24x7</b>           | <b>24x7</b>               | <b>24x7</b>               | <b>24x7</b>               | <b>24x7</b>               |
| Выявление инцидентов                                    |                       | <b>9x5</b>                | <b>24x7</b>               | <b>9x5</b>                | <b>24x7</b>               |
| Время обнаружения заведомо достоверного инцидента       |                       | <b>&lt; 15 мин.</b>       | <b>&lt; 15 мин.</b>       | <b>&lt; 15 мин.</b>       | <b>&lt; 15 мин.</b>       |
| Время обнаружения потенциального инцидента              |                       | <b>&lt; 30 мин.</b>       | <b>&lt; 30 мин.</b>       | <b>&lt; 30 мин.</b>       | <b>&lt; 30 мин.</b>       |
| Время подтверждения инцидента                           |                       | <b>до 2 час.</b>          | <b>до 2 час.</b>          | <b>до 2 час.</b>          | <b>до 2 час.</b>          |
| Расследование подозрений на инциденты                   |                       |                           |                           | +                         | +                         |
| <b>УПРАВЛЕНИЕ И ОТЧЕТНОСТЬ</b>                          |                       |                           |                           |                           |                           |
| Учет информации о критичных активах (CMDB)              | +                     | +                         | +                         | +                         | +                         |
| Предоставление отчетности                               | +                     | +                         | +                         | +                         | +                         |
| Управление инцидентами                                  |                       |                           |                           | +                         | +                         |
| Отчет по наиболее критичным событиям за прошедшие сутки | +                     | +                         | +                         | +                         | +                         |

\*Без ограничений в пределах согласованного порога по количеству событий в секунду (EPS) и при необходимости с использованием горизонтального масштабирования

Стоимость услуги зависит от выбранного уровня, дополнительных опций услуги и количества событий в секунду

