DATAPK

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ DATAPK

DATAPK

ОПИСАНИЕ DATAPK:

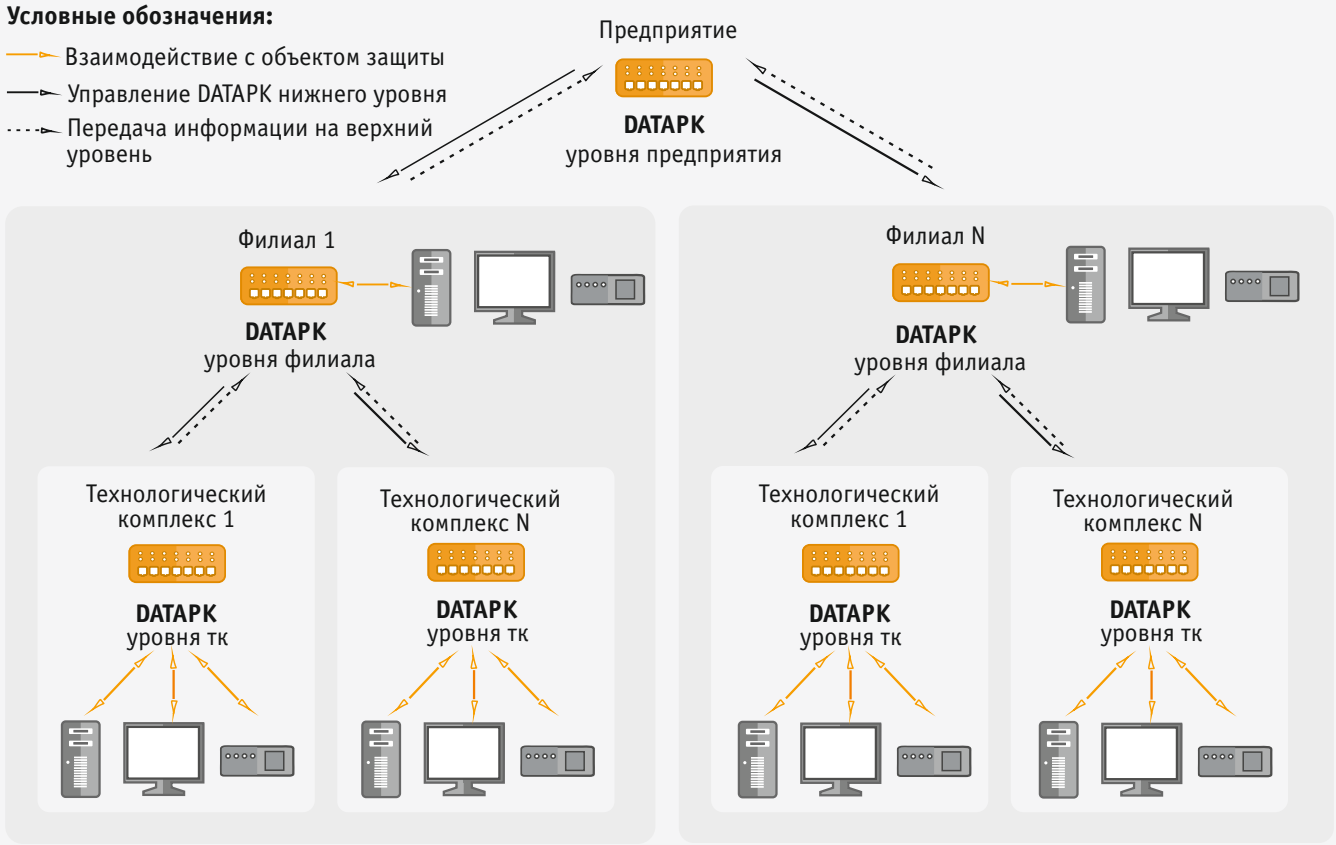
DATAPK – программно-аппаратный комплекс, обеспечивающий оперативный мониторинг и контроль состояния защищенности систем автоматизации критически важных объектов (КВО) и объектов критической информационной инфраструктуры (КИИ), в частности автоматизированных систем управления технологическими процессами (АСУ ТП).

РЕЖИМЫ РАБОТЫ DATAPK:

- **Пассивный мониторинг** - однонаправленное получение информации при отсутствии влияния на АСУ ТП.
- **Активный мониторинг** - обмен информацией с компонентами АСУ ТП с использованием штатных механизмов взаимодействия.
- **Сканирование защищенности** - активное взаимодействие с компонентами АСУ ТП с целью выявления уязвимостей

ОСОБЕННОСТИ DATAPK:

- **Безагентный сбор информации** – не требуется установка дополнительного ПО на компоненты АСУ ТП.
- **Настраиваемый сбор информации** – возможность самостоятельно настроить DATAPK для сбора конфигураций и событий со специфичных объектов защиты.
- **Различные варианты исполнения платформы,** в т. ч. промышленные – эксплуатация в расширенных температурных диапазонах, а также в условиях повышенной влажности и запыленности помещений.
- **Различные режимы работы** – функционирование в различных режимах в зависимости от степени критичности АСУ ТП и возможностей взаимодействия с ее компонентами.
- **Поддержка централизованного и локального управления** – возможность построения распределенных систем, используя механизм выстраивания иерархии DATAPK.
- **Интеграция с внешними системами управления ИБ** – интеграция в единую иерархическую систему мониторинга событий и инцидентов ИБ.
- **Наличие сертификата ФСТЭК** (№3731 от 12 апреля 2017 года) – подтверждение соответствия требованиям ТУ при выполнении указаний по эксплуатации, применение в качестве средства контроля (анализа) защищенности информации, не содержащей сведений, составляющих государственную тайну.



ИЕРАРХИЯ DATAPK:

В DATAPK реализован механизм, предоставляющий возможности по выстраиванию 3х уровней иерархии. Каждый уровень иерархии представлен отдельным вариантом исполнения DATAPK:

- **DATAPK уровня технологического комплекса** – обладает базовым набором функций по получению информации с объектов защиты технологического комплекса.
- **DATAPK уровня филиала** – обладает базовым набором функций, дополненным возможностью анализа событий безопасности и обработки конфигураций. Управляет подчиненными DATAPK уровня технологического комплекса.
- **DATAPK уровня предприятия** – обладает полным набором функций, включая оценку соответствия требованиям, выявление и анализ инцидентов. Управляет подчиненными DATAPK уровня филиала.

DATAPK

ХАРАКТЕРИСТИКИ DATAPK:

Характеристика	DATAPK		
	Технологический комплекс	Филиал	Предприятие
Объекты защиты			
Поддерживаемые объекты защиты	• ОС Microsoft Windows (начиная с Windows 98, NT 4.0). • ОС UNIX (в т. ч. Solaris, QNX, Linux и другие). • СУБД Microsoft SQL Server, MySQL, Oracle Database и другие. • Активное сетевое оборудование производства Cisco, HP, MOXA и другие. • SCADA-системы SIMATIC WinCC, Wonderware InTouch, ICONICS GENESIS и другие. • ПЛК производства SIEMENS, Allen-Bradley, Omron и другие		
Поддерживаемые протоколы в режиме индикации и сбора данных	SSH, SFTP, SCP, Telnet, MSRPC, HTTP(S), WinRM, Syslog, SMB (CIFS), NFS, FTP, SNMP, PROFINET, S7comm, протоколы передачи данных СУБД		
Поддерживаемые протоколы в режиме индикации	TPKT, COTP, OMRON FINS, IEC104, IEC 61850/MMS, Suitelink, MDLC, BSAP, Modbus RTU, OPC DA, проприетарный протокол Сириус-ИС и другие		
Режимы работы	• Пассивный мониторинг - однонаправленное получение информации при отсутствии влияния на АСУ ТП. • Активный мониторинг - обмен информации с компонентами АСУ ТП с использованием штатных механизмов взаимодействия. • Сканирование защищенности - активное взаимодействие с компонентами АСУ ТП с целью выявления уязвимостей и оценки		
Поддерживаемые функции			
Определение состава АСУ ТП	+	+	+
Определение информационных потоков	+	+	+
Обнаружение сетевых вторжений	+	+	+
Сбор и анализ конфигураций	+	+	+
Анализ защищенности, проверка соответствия требованиям ИБ	+	+	+
Сбор событий	+	+	+
Нормализация, корреляция событий, выявление инцидентов ИБ	–	+	+
Визуализация информации	–	+	+
Централизованное упр-е	–	–	+
Централизованное обновление	–	–	+
Характеристики базовой платформы			
Процессор	Intel Core i7, 2 ядра	Intel Xeon, 8 ядер	
Оперативная память	8 Гбайт	32 Гбайт	
Дисковая подсистема	512 Гбайт SSD	2x2 Тбайт, расширяемая	
Сетевые адаптеры	7x1 Гбит/с Ethernet	4x1 Гбит/с Ethernet	
Блок питания	60 Вт, внешний	Отказоустойчивое питание, 2x800 Вт	
Тип охлаждения	Пассивное	Активное	
Рабочая температура	-20..+70 °C	+10…+35 °C	
Сертификаты	RoHS, FCC, CE, EAC	RoHS, FCC, CE, EAC	
Размеры	125 мм x 210 мм x 77 мм	448,0 мм x 863,3 мм x 87,7 мм	
Монтаж	На стол, на стену VESA-75, на DIN-рейку	Монтажная стойка 19”	
Масса	1,9 кг	25 кг	
Особенности	Малогабаритная платформа промыш-го исполнения	Высокопроизводительная платформа уровня предприятия	