

ЧТО НОВОГО?

UDV DATAPK Industrial Kit 3.2





Введение	3
Общие обновления	4
• Поддержка ОС «Альт СП Сервер» 10.2.2 • Токены доступа для интеграции с внешними системами • Массовое назначение меток и АСУ ТП активам	
Модуль анализа промышленного сетевого трафика	6
• Детектирование индикаторов компрометации по репутационным спискам • Новые методы обнаружения угроз • Фильтрация по частичному совпадению домена в протоколе DNS • Обнаружение эксплуатации уязвимости Heartbleed • Расширена индикация протоколов	
Модуль контроля версий проектов ПЛК	9
• Поддержка TIA Portal V21 • Графическое сравнение версий проектов TIA Portal • Сопоставление версии проекта ПЛК в репозитории и на самом ПЛК	
Модуль управления уязвимостями	11
• Новый механизм поиска уязвимостей	
Контакты	12



UDV DATAPK Industrial Kit

UDV DATAPK Industrial Kit – это комплексное решение для обеспечения кибербезопасности любых АСУ ТП, которое позволяет быстро начать реагировать на угрозы без негативного влияния на защищаемые системы. Решение обеспечивает видимость ландшафта АСУ ТП, позволяет выявлять инциденты на ранних этапах, реагировать на них и выполнять требования регуляторов. UDV DATAPK Industrial Kit использует целостный подход и обширные возможности адаптации под нужды предприятия в рамках единого решения, что позволяет оптимизировать расходы на построение устойчивой защиты АСУ ТП.

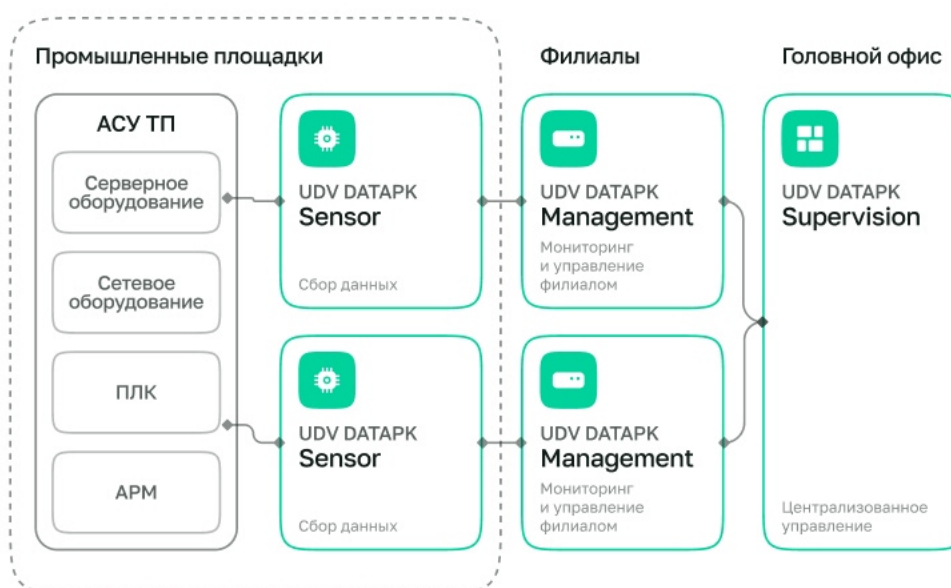


Рис. 1. Архитектурная схема UDV DATAPK Industrial Kit

Ключевые возможности

Анализ промышленного сетевого трафика (Industrial NTA)

Находит устройства внутри сети, быстро выявляет атаки и проводит расследования, контролирует параметры технологических процессов

Обнаружение аномалий для ПЛК (ML for PLC)

Оперативно выявляет аномалии в поведении ПЛК посредством безагентного анализа, используя методы машинного обучения

Контроль версий (Version Control)

Обеспечивает централизованное хранение проектов ПЛК, мониторит изменения и позволяет восстановить версии проектов, отслеживает неизменность программ на ПЛК

Управление уязвимостями (Vulnerability Management)

Проводит неинвазивный аудит защищенности АСУ ТП методом White Box, выявляет и позволяет устранить угрозы, проверяет соответствие требованиям ИБ

Управление конфигурациями (Configuration Management)

Контролирует соответствие необходимым значениям конфигураций любых ИТ и АСУ ТП устройств

Управление внешними событиями (External Events Management)

Собирает и обрабатывает события ИБ из различных внешних источников, визуализирует данные, позволяет отправлять нормализованные события в сторонние системы



Поддержка ОС «Альт СП Сервер» 10.2.2

В релизе 3.2 реализована поддержка новой версии операционной системы «Альт СП» 10.2.2 – это часть постоянной работы по поддержанию соответствия продукта требованиям сертификации регуляторов и по обеспечению долгосрочной технической поддержки.

Токены доступа для интеграции с внешними системами

Для подключения внешних систем к UDV DATAPK Industrial Kit по REST API реализована выписка токенов доступа - более безопасный и гибкий способ интеграции по сравнению с использованием общих учётных записей с постоянным паролем. Это упрощает работу с внешними системами оркестрации и другими средствами, с которыми планируется осуществить интеграцию.

The screenshot shows a web interface for managing access keys. At the top, there are navigation links: «Администрирование», «Пользователи», «Парольная политика», and «Ключи доступа». Below these is a section titled «Ключи доступа» with a count of 3 and a button «+ Создать ключ». A table lists existing keys with columns for Name, User, and Creation Date. A modal dialog titled «Ключ доступа создан» is open, displaying a generated key and instructions to copy it.

Наименование	Пользователь	Дата создания
NOC	Сумароков Александр Иванович (datapk)	24.09.2026, 12:57:38
semantix2	Сумароков Александр Иванович (datapk)	22.09.2026, 14:09:03
semantix	Сумароков Александр Иванович (datapk)	18.09.2026, 14:12:52

Ключ доступа создан

Скопируйте ключ и сохраните в безопасном месте. После закрытия окна посмотреть ключ будет нельзя.

YmRlYzYyNjMtNjdmYS00YTkyLTg0YjltZTQ2NmZlNjI5NGYzOjA4cTBWwWwzZmZQybR

Скопировать ключ Отменить

Рис. 2. Создание ключа доступа для интеграции с другой системой



Массовое назначение меток и АСУ ТП активам

Администраторы теперь могут выбрать группу объектов защиты, используя множественный выбор, и одним кликом назначить им метки или привязку к АСУ ТП. Это особенно удобно при развёртывании продукта на крупных промышленных площадках с сотнями объектов защиты, так как многократно сокращает время на первичную настройку системы по сравнению с разметкой каждого объекта отдельно.

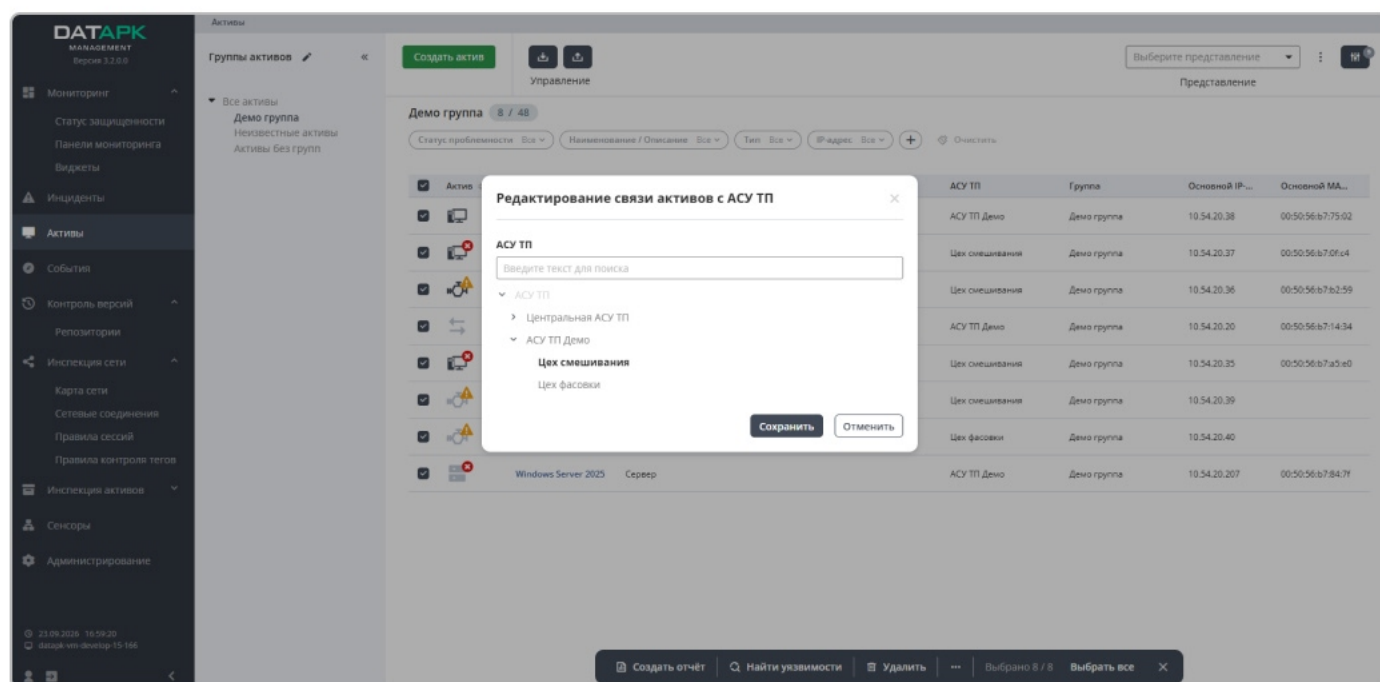


Рис. 3. Массовое добавление меток и редактирование АСУ ТП



Детектирование индикаторов компрометации
по репутационным спискам

В UDV DATAPK Industrial Kit 3.2 добавлена проверка трафика по репутационным спискам. Для всех клиентов с действующей лицензией на продукт становится доступна автообновляемая экспертиза вендора - UDV Threat Intelligence. Также возможно подключение собственной базы индикаторов компрометации заказчика.

Наименование	Индикатор	Тип	Сторона соединения	Источник	Описание	Дата обновл.	Дата добавл.	Активен
Malware payload...	15696	URL-адреса		UDV Group		23.09.2026, 16:06:17	17.09.2026, 10:29:46	Активный
Malware control ...	625	URL-адреса		UDV Group		23.09.2026, 16:06:17	17.09.2026, 10:29:47	Активный
Malware control ...	1577	IP-адреса	Отправитель ...	UDV Group		23.09.2026, 16:06:16	17.09.2026, 10:29:47	Активный
Malware control ...	3779	Доменные им...		UDV Group		23.09.2026, 16:06:16	17.09.2026, 10:29:46	Активный

Источник	Обновлено
UDV Group	23.09.2026, 16:06:18
Пользовательский	23.09.2026, 11:04:04

Рис. 4. Репутационные списки: пользовательские индикаторы и автообновляемый UDV Threat Intelligence

Продукт сверяет с репутационными списками IP-адреса участников соединений, доменные имена из DNS-запросов, URL из HTTP-запросов и хеши извлеченных из трафика файлов (MD5, SHA-256). Проверка учитывает направление взаимодействия - к активу или от актива - и сравнивает его с направлением, заданным для индикатора при загрузке списка. При совпадении по значению индикатора и направлению формируется событие ИБ. Учет направления резко снижает количество ложных срабатываний и помогает аналитику быстрее приоритезировать реагирование.

На ранних этапах атаки злоумышленники используют известную инфраструктуру и типовые инструменты - так дешевле, даже если канал управления зашифрован и содержимое недоступно для инспекции. Обращение к серверу из репутационного списка выдает атакующего. Проверка хешей файлов позволяет обнаружить известное вредоносное ПО, опираясь на многолетнюю экспертизу UDV Group в выявлении угроз для крупных российских промышленных предприятий.

Рис. 5. Совпадение с репутационным списком отображается прямо в карточке инцидента



Новые методы обнаружения угроз

Реализованы два новых механизма детектирования, увеличивающие точность обнаружения угроз:

1. Сигнатурный анализ с учетом границ контролируемой сети. В новом релизе правила срабатывают с учетом положения узла - внутри защищаемой инфраструктуры или за ее пределами. Раньше правила применялись ко всему трафику без разбора, и это порождало поток срабатываний, не имеющих отношения к реальным угрозам.
2. Переработанная логика обнаружения эксфильтрации данных через DNS-туннели - один из самых доступных каналов скрытой передачи данных, поскольку DNS-трафик разрешен практически в любой сети.

Оба метода делают срабатывания более точными и релевантными для конкретной инфраструктуры заказчика, снижая нагрузку на аналитиков ИБ: теперь специалисты видят меньше нерелевантных событий и быстрее доходят до реальных угроз.

Фильтрация по частичному совпадению домена в протоколе DNS

В фильтре по доменному имени добавлен поиск по частичному совпадению — по аналогии с фильтром «Приложение клиента» в протоколе HTTP.

Вредоносные домены и DNS-туннели часто меняют только один из уровней доменного имени. Поиск по полному совпадению в таких случаях не работал: аналитику приходилось перебирать варианты вручную. Теперь достаточно указать неизменную часть домена, чтобы увидеть всю связанную активность.

Обнаружение эксплуатации уязвимости Heartbleed

В релизе 3.2 добавлено обнаружение попыток эксплуатации известной уязвимости Heartbleed (CVE-2014-0160), она по-прежнему встречается на необновлённом оборудовании и во встраиваемых системах, распространённых в промышленных сетях.

Heartbleed (CVE-2014-0160) - это уязвимость в библиотеке Open SSL, позволяющая злоумышленнику читать память сервера и похищать закрытые ключи, учетные данные и содержимое сессий.



Расширена индикация протоколов

Комплекс теперь распознаёт больше протоколов, важных для контроля промышленных и корпоративных сетей:

- Modbus RTU over TCP - к уже поддерживаемому разбору Modbus добавлена индикация его инкапсуляции внутри TCP. Наличие в сети этого варианта протокола указывает на нестандартную схему подключения АСУ ТП-оборудования и риск некорректного сегментирования сети;
- Regul - добавлен разбор команд управления Start, Stop, Load, что позволяет фиксировать в трафике операции запуска, остановки программы и загрузки программы на контроллере;
- SSDP, mDNS, LLNMR - эти протоколы обнаружения устройств злоумышленники используют для перехвата учетных данных (LLMNR/NBT-NS poisoning), а их видимость помогает найти неучтенные устройства в сети: например, принтеры, IoT-оборудование, которые обычно не проходят инвентаризацию;
- RTSP - контроль видеопотоков, обнаружение камер и регистраторов в неожиданных сегментах сети;
- PTP - видимость трафика точной синхронизации времени в промышленных и телеком-сетях;
- Zabbix (agent, trapper) - контроль трафика систем мониторинга и выявление нелегитимных подключений под видом служебного трафика.

Это расширяет применимость продукта на разнородных промышленных объектах и помогает выявлять неучтённое оборудование в сети - от камер видеонаблюдения до IoT-устройств.



Модуль контроля версий проектов ПЛК в составе UDV DATAPK Industrial Kit — это единственное на рынке РФ решения для централизованного хранения и управления версиями проектов ПЛК, сертифицированное ФСТЭК России.

Поддержка TIA Portal V21

В версии 3.2 реализована поддержка TIA Portal V21 — самой актуальной версии среды разработки Siemens на момент релиза, что позволяет заказчикам работать с новейшими линейками и проектами ПЛК Siemens.

Графическое сравнение версий проектов TIA Portal

Реализовано визуальное сравнение изменений между версиями проекта ПЛК на языках LAD, FBD, SCL и ST.

Раньше инженеру приходилось анализировать различия в текстовом или структурном виде, теперь изменения в логике управления показываются графически так же, как инженер видит их в самой среде разработки. Это значительно упрощает контроль изменений и снижает риск незамеченных модификаций в критичной логике управления технологическим процессом.

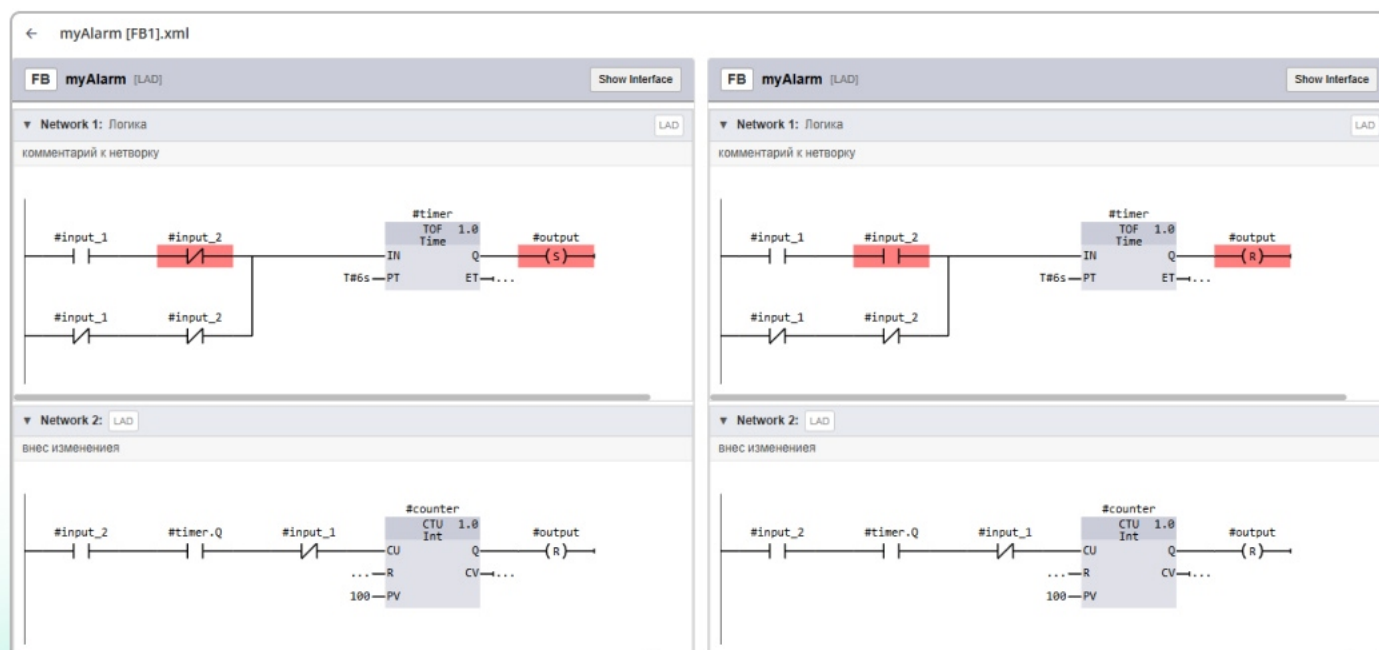


Рис. 6. Графическое сравнение версий проектов Siemens: отображение изменений для блока FB1



Сопоставление версии проекта ПЛК в репозитории и на самом ПЛК

В части управления версиями проектов ПЛК важно не только знать, какая версия считается эталонной и где она хранится, но и быть уверенным, что именно она загружена на ПЛК.

В релизе UDV DATAPK Industrial Kit для контроллеров Siemens появилась функциональность сопоставления версии проекта ПЛК в репозитории и на самом ПЛК, в том числе - возможность настроить эту сверку по расписанию.

Агрегат 1

Версии проекта 6

Содержание проекта

Активы 1

Путь к локальной версии

C:\Users\user\Documents\Automation\...

Группа объектов

Демо-зона

Описание репозитория

—

Размер проекта

11.3MB

Опрос ПЛК

Совпадает: 1

24.08.2026, 16:28:39

Серверная версия

6. 5502dafd

от 26.06.2026, 12:36:35

Локальная версия

6. 5502dafd

от 26.06.2026, 12:36:35

№	Версия	Изменена	Автор	Обоснование изменений	Описание изменений
6	5502dafd	26.06.2026 12:36:35	Иванов Иван	Демо	Изменения в логике
5	c9b17ece	17.06.2026 12:27:49	Иванов Иван	Демо	Alarm block
4	aa187223	16.06.2026 18:01:02	Иванов Иван	Корректировка LAD-блока	Откорректирован блок, изменен ...

Рис. 7. Сопоставление версии проекта в репозитории с версией, загруженной на ПЛК

Прочие обновления

В интерфейсе Desktop App появилось отображение IP-адреса управляющего комплекса. Это удобно в технологических сегментах сети, где DNS настроен не всегда, и инженеру важно быстро увидеть, к какому серверу подключено рабочее место.

Проверить актуальность данных

0 минут назад

Подключено к серверу

datapk-ivanovm | 10.51.20...

datapk

demo_v17

Версии проекта 12

Содержание проекта

Активы 1

Путь к локальной версии

C:\Users\user\Documents\Automation\...

Группа объектов

plc_programs / TIA

Описание репозитория

—

Размер проекта

14.2MB

Опрос ПЛК

Не совпадает: 1

18.09.2026, 12:48:54

Серверная версия

12. dd7f62b5

от 18.09.2026, 12:48:23

Локальная версия

12. dd7f62b5

от 18.09.2026, 12:48:23

Рис. 8. Отображение IP-адреса управляющего комплекса



Новый механизм поиска уязвимостей

В релизе UDV DATAPK Industrial Kit 3.2 поиск уязвимостей ведется по следам ОС и ПО.

Новый механизм охватывает значительно более широкий круг оборудования, включая нетиповое промышленное оборудование, для которого прежний инструмент на базе стандарта OVAL не поддерживал сбор данных об уязвимостях. Данный подход дает более точную и полную картину уязвимостей без избыточной сетевой нагрузки на проверяемые узлы.

**Закажите пилотный проект
или персональную демонстрацию
наших решений**



Контакты

zapros@udv.group
8-800-511-65-51

Сайт

udv.group

Телеграм

@udv_group

Адрес

620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4 udv.group