ALD Pro

ИНТЕГРАЦИЯ С ДРУГИМИ СИСТЕМАМИ И СЕРВИСАМИ

06.08.25

АСТРА

Astra Disk

Astra Disk — это российская платформа для организации хранения, совместной работы и обмена документами разных форматов внутри компании.

Интеграция позволяет:

- Импортировать пользователей и группы из домена, даёт возможность аутентификации и авторизации пользователей с использованием доменных учётных записей, а также чтобы использовать эту информацию для разграничения прав доступа.

Интеграция реализована через LDAP-коннектор.

RuPost

RuPost — это корпоративная почтовая система с календарями, задачами, адресными книгами и другими функциями, важными для компаний. RuPost содержит в своем составе графический инструмент миграции с MS Exchange, позволяющий поэтапно и гранулярно перенести почтовые данные, календари, контакты, общие ящики и архивы, а также права доступа между пользователями.

RuPost использует серверы LDAP для аутентификации и получения данных о пользователе из каталога, поэтому интеграция:

- Не требует расширения схемы LDAP (версии ALD Pro 1.3.x и выше);
- Содержит скрипт rupostadmin для управления сервисными учетными записями RuPost.

RuBackup

RuBackup - решение для автоматизированной защиты данных инфраструктурных систем любого масштаба и бизнес-приложений.

Интеграция позволяет:

- Обеспечить аутентификацию по протоколу LDAP/LDAPS через службу каталога ALD Pro. Благодаря интеграции с RuBackup вы можете снимать копию каталога либо всего КД целиком.

Уже в ближайшее время запланирована интеграция на уровне агентов для резервного копирования контроллеров и подсистем.

АСТРА

Tantor

Tantor – это веб-портал для эффективного управления экземплярами СУБД Tantor и PostgreSQL. Платформа позволяет снизить эксплуатационные расходы по управлению базами данных, основанных на PostgreSQL.

Интеграция позволяет:

- Импортировать пользователей и группы из домена, чтобы использовать эту информацию для разграничения прав доступа к тенантам и рабочим пространствам. Аутентификация доменных пользователей проводится методом LDAP Bind.

Интеграция реализована посредством LDAP-коннектора.

GitFlic

GitFlic – российская платформа для разработчиков, сочетающая в себе необходимые инструменты для работы как для больших компаний и команд, так и для частных пользователей.

Интеграция позволяет:

- Выполнить импорт пользователей, привязать их к учетным записям из домена и обеспечить аутентификацию через единую точку входа по протоколам LDAP или Kerberos V5. Для назначения прав доступа можно использовать информацию об участии доменных пользователей в группах, для чего нужно настроить сопоставление локальных и доменных групп.

Брест

ПК СВ "Брест" - российская платформа со встроенными средствами защиты информации серверной ОС Astra Linux Special Edition для создания и управления облачными виртуальными ИТ-инфраструктурами.

Интеграция позволяет:

- Обеспечить аутентификацию доменных пользователей в веб-интерфейсе системы Брест по безопасному протоколу Kerberos V5. Если у пользователя еще нет аккаунта в системе виртуализации Брест, но пользователь является участником доменной группы brestadmins или brestusers, то после успешной аутентификации аккаунт будет создан автоматически.

Astra Monitoring

Astra Monitoring - отечественная система мониторинга ИТ-инфраструктуры, обеспечивающая контроль состояния серверов, рабочих станций и сетевого оборудования.

Интеграция позволяет:

- Организовать централизованную аутентификацию пользователей через LDAP без создания отдельных учётных записей в системе мониторинга. Для подключения используется сервисная учётная запись и защищённый протокол LDAPS. Авторизация и распределение прав внутри Astra Monitoring настраиваются локально.

1С – это платформа, на которой работает огромное количество популярных систем учёта, автоматизирующих расчёт заработной платы, управление активами, управление финансами, ведение управленческого учёта и др.

Интеграция позволяет:

- Обеспечить единую точку входа по протоколу Kerberos V5. Поддерживаются все типы клиентских приложений: тонкие, толстые и веб. Информация об участии пользователей в группах не используется, авторизация настраивается исключительно средствами 1С.

  В настоящий момент работа в доверительных отношениях не поддерживается клиентом 1С, сервер необходимо присоединить к домену ALD Pro.

Яндекс 360

Яндекс 360 – это платформа для организации совместной работы сотрудников предприятия, включающая в себя корпоративную почту, календарь, мессенджер, общий доступ к файлам, документы и др.

Интеграция позволяет:

- Предоставить авторизованный доступ к сервисам пользователей домена. Механизм аутентификации работает с помощью Keycloak по протоколу SAML.

  Сервер Keycloak можно установить из приложения, доступного в Яндекс облаке как сервис.

Битрикс24

Битрикс 24 – это платформа для построения корпоративных порталов и создания веб-сайтов организации.

Интеграция позволяет:

- Импортировать пользователей, привязать их к учетным записям из домена.
- Обеспечить аутентификацию через единую точку входа по протоколам LDAP или Kerberos V5.
- Использовать информацию об участии доменных пользователей в группах для назначения прав доступа (необходимо настроить сопоставление локальных и доменных групп).

МТС ЛИНК

МТС Линк – это экосистема сервисов для онлайн-коммуникаций и совместной работы. Экосистема включает в себя решения для проведения онлайн-встреч и совещаний, вебинаров, крупных виртуальных и гибридных мероприятий, создания собственных курсов, интерактивных онлайн-досок и чаты для оперативного общения.

Интеграция позволяет:

- Упростить администрирование сервиса МТС Линк, для предоставления доступа к системе пользователя достаточно включить в соответствующую доменную группу. При входе в систему пользователю нужно ввести логин/пароль от своей доменной учётной записи, аутентификация и авторизация выполняется с помощью LDAP-коннектора.

Аладдин

Аладдин – удостоверяющий центр от российского разработчика, с помощью которого можно построить на предприятии инфраструктуру открытых ключей (PKI).

Интеграция позволяет:

- Автоматизировать выдачу ключей за счёт получения информации о сотрудниках из каталога. Открытый ключ может быть автоматически записан в учётную запись пользователя для обеспечения двухфакторной аутентификации по сертификату с использованием смарт-карт или USB-токенов JaCarta. Аутентификация выполняется с помощью клиентского приложения для входа SecurLogon по протоколу Kerberos V5 с использованием расширения PKINIT.

Kaspersky Unified Monitoring and Analysis Platform

MaxPatrol SIEM

SIEM (Security Information and Event Management) — это система управления информационной безопасностью и событиями безопасности. Она позволяет организациям обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб.

Совместно с разработчиками ведущих SIEM-систем был проанализирован технологический стек компонентов службы каталога ALD Pro для правильной настройки функции аудита с учётом их многолетнего опыта работы со службой каталога MS AD.
Коллеги из SIEM-команд подготовили комплекты экспертизы для нормализации этих событий и автоматического выявления возможных инцидентов безопасности (корреляции). Интеграция службы каталога с SIEM-системой значительно повышает безопасность ИТ-инфраструктуры.

SafeTech CA

SafeTech CA — современный отечественный центр сертификации, который способен полностью заменить Microsoft CA и оптимизировать процессы выпуска и управления жизненным циклом сертификатов.

Интеграция позволяет:

- Обеспечить выпуск сертификата для доменного пользователя. База пользователей и информация о них читается из каталога через протокол LDAP. Данные сертификаты можно использовать в любых сервисах для авторизации пользователя, которые настроены на доверие к этому CA.

В будущем планируется развитие интеграции по 2 направлениям:
1. Центр сертификации для домена, который будет выписывать сертификаты по запросу от ALD Pro при создании пользователей или развертывании подсистем.
2. Реализация системы для доменной двухфакторной аутентификации на базе электронных подписей под управлением CA.

Ankey IDM

Ankey IDM — программный продукт для централизованного управления учётными записями пользователей и их полномочиями в корпоративных информационных системах.

В системе Ankey IDM реализован LDAP-коннектор, с помощью которого возможно управление объектами службы каталога, такими как пользователи, группы пользователей и организационные подразделения, на основе информации из доверенного источника, в роли которого может выступать система управления кадрами. Продукт Ankey IDM позволяет организовать рабочие процессы по согласованию заявок на предоставление доступа (включение в группы безопасности) службе каталога, что существенно повышает безопасность инфраструктуры.

ORIONsoft Termit

Termit – система организации терминального доступа для удаленной работы, в том числе через каналы передачи данных низкого качества и с устаревшим ПК. Российская разработка с собственным движком и кодовой базой без основы из Open Source.

Интеграция позволяет:

- Организовать вход пользователей на портал администратора и терминальные серверы через доменные учетные записи по протоколам LDAP и Kerberos V5.

BASIS

Базис.Virtual Security – это сертифицированное ФСТЭК РФ средство защиты информации систем виртуализации и облачных платформ.

Интеграция позволяет:

- Настроить единую точку входа (Single Sign-On, SSO), при которой пользователи могут аутентифицироваться один раз и получать доступ к нескольким приложениям или сервисам без необходимости повторного ввода учетных данных.
- Появляется возможность централизованного управления пользователями, ролями и правами доступа.
- Решение позволяет настраивать различные сценарии аутентификации, включая многофакторную аутентификацию (MFA), условный доступ и кастомизацию форм входа.

PROXMOX

Proxmox - система виртуализации, которая даёт возможность создания и управления виртуальными машинами через веб-интерфейс либо через стандартный интерфейс командной строки Linux.

Интеграция позволяет:

- Централизованно вести базу пользователей, аутентифицировать и авторизовывать пользователей через ALD Pro, а также управлять их доступами путем изменения членства в группах.

  Модель безопасности при этом должна быть предварительно настроена на Proxmox VE. Интеграция выполняется методом LDAP Bind через сервисную учетную запись.

DirectumRX

Directum RX является расширяемой системой электронного документооборота, которая является очень гибкой и позволяет реализовать любую логику бизнес-процессов.

Интеграция позволяет:

- Выполнять аутентификацию в сервисе Directum RX от имени доменного пользователя. Для настройки аутентификации необходимо создать пользователя в Directum RX и связать его с доменным (информация о котором будет получена из TGS-билета Kerberos). Таким образом, сейчас возможно настроить работу в Directum RX для доменных пользователей с использованием доменной SSO Kerberos без необходимости ввода пароля, но настраивать каждого пользователя придется вручную.

Интеграция ALD Pro и Directum RX выполнена на уровне аутентификации через Kerberos.

DION

DION – это платформа для организации корпоративных коммуникаций, включающая видеоконференции, видеохостинг, переговорные комнаты, звонки, вебинары и чаты.

Интеграция позволяет:

- Осуществить извлечение информации о пользователях и группах службы каталога по протоколу LDAP. Аутентификация пользователей выполняется по безопасному протоколу SAML.

ELMA365

ELMA365 представляет собой облачное решение для управления бизнес-процессами, построенное на принципах Low-code разработки, что позволяет максимально быстро превращать бизнес-идеи в работающие цифровые решения.

Интеграция позволяет:

- Обеспечить автоматическую синхронизацию пользователей и групп, а также безопасную аутентификацию доменных пользователей через защищенный протокол LDAPs.

Благодаря встроенному LDAP-модулю система легко интегрируется с ALD Pro.

Exchange

Exchange - платформа для организации корпоративной email-системы и коллективной работы сотрудников. Решение предоставляет совместный доступ к задачам и календарям.

Интеграция через механизм связанных почтовых ящиков дает пользователям из домена ALD Pro следующие возможности:

- Иметь почтовые ящики в MS Exchange;
- Аутентифицироваться и авторизовываться в MS Exchange с использованием учетных данных из ALD Pro;
- Управлять своим почтовым ящиком, меняя данные в профиле почтового ящика;
- Пользоваться полным функционалом почтового сервера, отправлять и получать письма, делегировать почтовый ящик, участвовать в списках рассылки и многое другое.

OPEN VPN - серверное приложение, позволяющее обеспечить доступ удалённых сотрудников к локальной сети предприятия по технологии виртуальной частной сети (VPN) с использованием шифрованных каналов связи.

Интеграция позволяет:

- Реализовать возможность пользователям устанавливать защищённые VPN-соединения с использованием доменных учётных записей. Пароль на VPN-сервер предоставляется в открытом виде, проверка выполняется через службу SSSD по протоколу Kerberos V5, как при интерактивном входе в систему.

  Доступ можно настроить с учётом участия пользователя в группах, в том числе с использованием HBAC-правил.

KEYCLOAK - продукт с открытым кодом для реализации единой точки входа (англ. Single Sign-On, SSO).

Интеграция позволяет:

- Предоставить доменным пользователям возможность аутентификации в веб-приложениях по современным протоколам OAuth2, OpenID, SAML.

Интеграция с ALD Pro реализована через LDAP-коннектор.

ViPNet SafeBoot - это программный модуль доверенной загрузки. Он может блокировать загрузку еще на стадии UEFI и разрешать ее только тем пользователям, которые смогут пройти аутентификацию с помощью учетной записи из домена ALD Pro.

Интеграция позволяет:

- Осуществлять аутентификацию пользователей ALD Pro по протоколу LDAP еще на стадии загрузки UEFI.

Поддержка ALD Pro реализована в версии ViPNet SafeBoot 3.0.1.

Pro32connect – это программное обеспечение для удаленного доступа к рабочему столу из браузера. Предназначено для профессионального использования: системного администрирования и технической поддержки.

Интеграция позволяет:

- Обеспечить аутентификацию и авторизацию пользователя в системе, а также позволяет разграничивать права пользователей при помощи членства в группах каталога.

Solar inRights

Solar inRights — это современная система управления учётными данными (англ. Identity Governance Administration, IGA), автоматизирующая процесс управления жизненным циклом учётных записей пользователей в информационных системах предприятия. Источником доверенной информации для Solar inRights является кадровая информационная система, а с системой ALD Pro продукт интегрирован с помощью коннектора, который написан на языке Java и взаимодействует с каталогом через API-запросы по протоколу HTTPS.

Интеграция позволяет:

- Создавать, изменять, удалять учётные записей пользователей, групп, структурных подразделений;
- Устанавливать пользователю пароль;
- Активировать/деактивировать пользователей и др.

SafeConnect

SafeConnect – это веб-портал, с помощью которого пользователям можно предоставить доступ к корпоративным приложениям из веб-браузера. На данный момент в систему уже встроены следующие клиентские приложения: RDP, RDP app, VNC, SSH, Telnet, HTTP(S).

Интеграция позволяет:

- Пользователям проходить аутентификацию с использованием своих доменных учётных записей. При публикации приложений администраторы могут предоставлять доступ пользователям с учётом информации об их участии в группах.

Интеграция с ALD Pro реализована посредством LDAP-коннектора.
Продукт может работать совместно с SafeInspect.

Solar SafeInspect

Solar SafeInspect — это система для управления привилегированным доступом (англ. Privileged Access Management, PAM), которая позволяет проксировать удалённые подключения привилегированных администраторов к серверам по протоколам SSH, RDP и др., обеспечивая детальный контроль, мониторинг и аудит выполняемых действий с возможностью принудительного прерывания сессии.

Интеграция позволяет:

- Настроить аутентификацию привилегированных пользователей с использованием учётных данных из домена ALD Pro. В дополнение к этому система позволяет использовать информацию об участии пользователей в доменных группах для распределения прав доступа и настройки правил аудита.

Solar Dozor

Solar Dozor — это система корпоративного класса для предотвращения утечек данных (англ. Data Leak Prevention, DLP). Она обеспечивает контроль коммуникаций сотрудников, блокировку отправки нежелательных сообщений, выявление групп риска и мониторинг их активностей. Система позволяет также делать ретроспективный анализ по архиву коммуникаций.

Интеграция позволяет:

- Синхронизировать данные каталога с внутренней базой объектов Dozor. Аутентификация доменных пользователей в консоли управления системой возможна по безопасному протоколу Kerberos V5.

Интеграция реализована посредством LDAP-коннектора.

Ideco NGFW – это межсетевой экран, который обеспечивает защиту внутреннего периметра сети на разных уровнях и позволяет управлять доступами во внешнюю сеть для конкретных пользователей и/или групп. Помимо этого, возможно выполнить настройку правил доступа из внешней сети в локальную.

Интеграция позволяет:

- Вести базу пользователей централизованно, а также перенести функционал аутентификации и авторизации на ALD Pro, включая аутентификацию посредством Kerberos. Это позволит пользователям прозрачно авторизоваться на Ideco NGWF и получать доступы в соответствии с правилами на Ideco. Интеграция выполняется путем создания учётной записи Ideco в домене ALD PRO и поддерживает протокол Kerberos.

Printum – это система мониторинга и управления печатью, повышающая эффективность использования принтеров и МФУ на предприятиях. Позволяет создавать правила, запрещающие печать больших документов на устройствах с низкой производительностью, устанавливать квоты на цветную печать, удалять неактуальные задания, настраивать двустороннюю печать и экономию тонера.

Интеграция позволяет:

- Импортировать пользователей и группы из домена и использовать эту информацию для настройки правил системы.

MikoPBX - это бесплатный сервер телефонии с операционной системой и веб-интерфейсом.

Интеграция позволяет:

- Синхронизировать пользователей системы с учетными записями каталога.

Интеграция с ALD Pro реализована по протоколу LDAP.

Р7 - Офис (Корпоративный сервер) — профессиональные онлайн и оффлайн инструменты для работы с документами и контентом. Единое пространство для хранения и управления документами организации, планирования, взаимодействия сотрудников и контрагентов.

Интеграция позволяет:

- Настроить синхронизацию пользователей и групп для последующей аутентификации в системе Р7 посредством LDAP Bind.

.

Pragmatic Tools

Pragmatic Tools Migrator — это инструмент, автоматизирующий миграцию из Microsoft Active Directory в каталоги производителей отечественных операционных систем, такие как ALD Pro от Astra Linux.

Интеграция позволяет:

- Обеспечить бесшовную миграцию данных в службу каталога ALD Pro и работу в гибридных инфраструктурах. В ALD Pro уже есть модуль синхронизации, который имеет функциональность, схожую с Pragmatic Tools Migrator, и закрывает потребности большинства заказчиков. Вместе с тем, если вам понадобится не только сопоставление атрибутов, но и трансформация данных, то с такой задачей поможет справиться решение наших коллег Pragmatic Tools Migrator. С его помощью, например, можно добавить суффиксы к именам учетных записей, чтобы обеспечить их уникальность при миграции пользователей из нескольких доменов Active Directory сразу.

Granulex

Granulex Recovery – предназначен для быстрого исправления логических ошибок в LDAP-каталоге и отката ошибочных или нежелательных изменений. В отличие от классического восстановления из бэкапа, Granulex Recovery позволяет восстановить необходимые данные всего за несколько минут.

Интеграция позволяет:

- Оперативно сравнивать текущее состояние каталога с информацией из резервной копии и восстанавливать отдельные записи и атрибуты, что дает неоспоримые преимущества по сравнению с полным восстановлением LDAP-каталога из бэкапа. Комплексное внедрение решений ALD Pro и Granulex Recovery упрощает управление каталогом как на этапе первичной миграции из MS Active Directory, так и в процессе дальнейшей эксплуатации на малых и средних предприятиях.

КонсультантПлюс

Консультант плюс - это российская правовая информационно-аналитическая система, предоставляющая доступ к актуальным данным о законодательстве, нормативных актах, судебной практике и комментариям экспертов. Система устанавливается внутри предприятия и доступна пользователям из браузера по протоколу HTTP.

Интеграция позволяет:

- Реализовать централизованное управление лицензиями, доступ к приложению получают только авторизованные пользователи, которые были включены в специальную доменную группу.

Гарант

ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

Гарант – это информационно-правовая система для решения профессиональных задач юриста, бухгалтера, кадровика, специалиста по закупкам с актуальной информацией и широким функционалом для оперативного поиска и анализа материалов. Система устанавливается внутри предприятия и доступна пользователям из браузера по протоколу HTTP.

Интеграция позволяет:

- Обеспечить прозрачную аутентификацию доменных пользователей по безопасному протоколу Kerberos V5.
- Для возможности централизованного управления лицензиями доступ к приложению получают только авторизованные пользователи, которые были включены в специальную доменную группу.

«Штурвал» — отечественная платформа для управления контейнерами от компании «Лаборатория Числитель». Решение позволяет автоматизировать развёртывание, управление и мониторинг контейнеризованных приложений на базе технологии Kubernetes. Подходит как для крупных предприятий, так и для небольших организаций.

Интеграция позволяет:

- Платформе Штурвал использовать сервер LDAP для аутентификации и получения базовых данных о пользователе из каталога.

.

Foreman - это открытый инструмент для взаимодействия с Puppet (или Chef), позволяющий автоматизировать выполнение задач и развёртывание приложений.

Интеграция позволяет:

- Обеспечить возможность сопоставления доменных учетных записей с пользователями Foreman для аутентификации по протоколам LDAP и Kerberos V5 при авторизации в веб-интерфейсе.

UserGate NGFW – это межсетевой экран, обеспечивающий высокий уровень защиты от угроз для сетей любого формата и размера благодаря максимальной видимости событий безопасности, совмещает в себе систему обнаружения вторжения и межсетевой экран.

Интеграция позволяет:

- Получать информацию о пользователях и группах домена и использовать эти данные при настройке правил фильтрации и разграничении доступа.
- Прозрачно аутентифицировать пользователей посредством протокола Kerberos.
- Предоставлять пользователям или группам домена административный доступ к UserGate NGFW.

1IDM — это IDM-система, построенная на платформе 1С и предназначенная для интеграции бизнес-процессов из 1С с внешними сервисами предприятия.

Интеграция позволяет:

- Централизованно управлять пользователями домена: создавать и блокировать учётные записи, изменять атрибуты, управлять членством в группах и назначать роли. Взаимодействие реализовано через REST-API ALD Pro, что обеспечивает гибкую и автоматизированную синхронизацию между системами.

Пассворк

Пассворк — это менеджер паролей, упрощающий совместную работу с корпоративными учётными данными. Все пароли безопасно хранятся на вашем сервере, сотрудники быстро находят нужную информацию, а администратор управляет правами доступа и отслеживает все действия и изменения.

Интеграция позволяет:

- Интеграция доступна только в Расширенной лицензии Пассворк. Она позволяет настроить синхронизацию пользователей и групп для последующей аутентификации в системе Пассворк посредством LDAP Bind.
- В облачной версии Пассворк поддержка LDAP не предусмотрена — интеграция возможна только при локальном развертывании.

MAKVES DCAP

Makves DCAP - это система аудита и контроля доступа к информации, обеспечивающая централизованный сбор, анализ и хранение событий безопасности в корпоративной сети.

Интеграция позволяет:

- Автоматически получать события аутентификации, изменения объектов каталога, администрирования и прочих критически важных действий, происходящих в доменной среде.
- Интеграция реализуется без установки дополнительных агентов на ALD Pro, что упрощает развёртывание и снижает нагрузку на инфраструктуру. Настройка экспорта событий осуществляется с помощью syslog-ng, что позволяет гибко управлять источниками логов и маршрутами доставки.

MFASOFT

Secure Authentication Server (SAS) от MFASOFT - отечественное решение для организации многофакторной аутентификации, обеспечивающее дополнительный уровень защиты при входе в корпоративные системы за счёт использования одноразовых паролей, токенов и других методов подтверждения личности.

Интеграция позволяет:

- Использовать доменные учётные записи для единой аутентификации через LDAP и Kerberos, обеспечивая централизованное управление пользователями и настройку многофакторной аутентификации без дублирования данных. Это повышает безопасность и удобство доступа к корпоративным ресурсам.

TrueConf

TrueConf - это платформа для корпоративной видеосвязи и проведения защищённых видеоконференций.

Интеграция позволяет:

- Централизованно управлять доступом пользователей, выполнять их импорт через LDAP и обеспечить аутентификацию по Kerberos V5 с использованием технологии единого входа (SSO).
- Интеграция поддерживает фильтрацию по группам, отображение дополнительных атрибутов и настройку зон с различными способами аутентификации. TrueConf Server можно включить в домен ALD Pro и использовать keytab-файл для настройки Kerberos SSO без ввода логина и пароля.

ZABBIX

Zabbix — это система мониторинга, предназначенная для сбора, анализа и визуализации данных о состоянии IT-инфраструктуры: серверов, сетевого оборудования, приложений и сервисов.

Интеграция позволяет:

- Настроить аутентификацию пользователей через защищённое соединение по протоколу LDAPS. Это обеспечивает безопасный доступ к Zabbix с использованием доменных учётных записей и централизованного управления пользователями. Возможна привязка ролей и прав доступа на основе членства в группах домена.
- Интеграция упрощает администрирование и позволяет использовать единые учётные данные без необходимости ручного создания и поддержки отдельных аккаунтов в системе мониторинга.

СПАСИБО ЗА ВНИМАНИЕ!