УТВЕРЖДАЮ:
ДИРЕКТОР ЧТПУП «ГРАНКОМ»

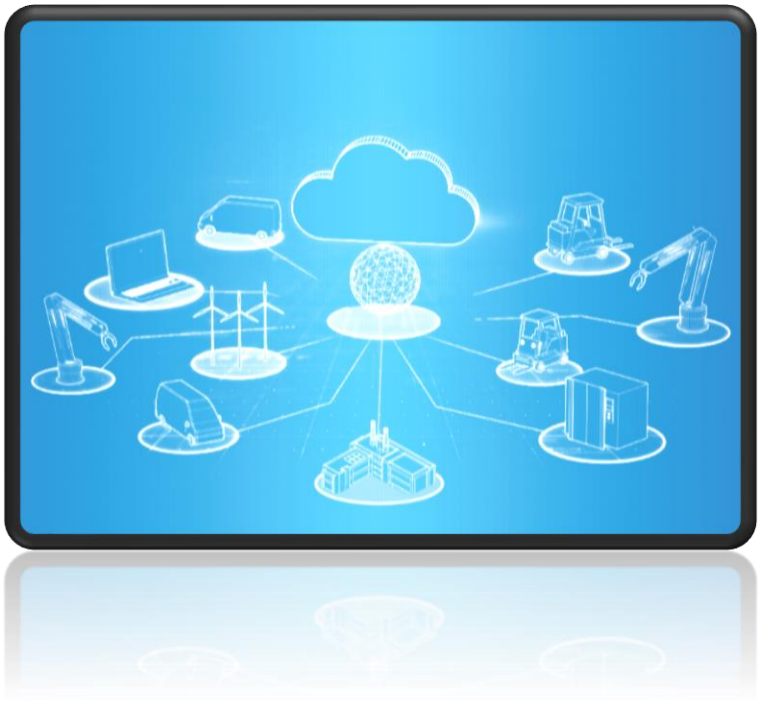
Готовко Д.О

ГЛОИС

ТЕХНИЧЕСКИЕ УСЛОВИЯ ПОДКЛЮЧЕНИЯ

на 10 листах

(v01.0:16/03/2017)



МИНСК, БЕЛАРУСЬ

Содержание

1. Основные положения

ГЛОИС разработана для создания «единой точки доступа» ко всей инженерно-технической инфраструктуре объекта. Она позволяет контролировать любую интегрированную систему, или устройство в пределах системы, с локальных и удаленных рабочих мест, независимо от размера объекта — от одного здания до решений городского или регионального масштаба.

Настоящие технические условия распространяются на Систему ГЛОИС, предназначенную для реализации сервиса on-line взаимодействия пользователей с компонентами клиентских объектов.

Средой взаимодействия пользователей является графический интерфейс сайта ГЛОИС (далее – графический интерфейс), который предназначен для автоматизации предоставления услуг по мониторингу и управлению клиентскими объектами.

Посредством графического интерфейса реализуется:

- Полная ситуационная картина оперативной обстановки на объектах мониторинга в рамках предварительно настроенных полномочий;
- Качественная визуализация различных типов данных, поступающих от всех интегрированных систем: видео- и аудиоданные, события, команды, переменные;
- Управление устройствами, системами клиентских объектов;
- Визуализация взаимодействия всех элементов интегрированных систем;
- Создание аналитических отчетов.

1.1. Область применения

1.2. Условия эксплуатации

ГЛОИС функционирует в режиме 24/7/365 (24 часов в сутки, семь дней в неделю и круглогодично).

1.3. Общее описание информационного обмена

Обмен данными между компонентами ГЛОИС (облачный сервис, контроллеры передачи данных, конечные устройства) осуществляется с использованием сети Интернет. При осуществлении информационного обмена основными сетевыми телекоммуникационными протоколами являются протоколы семейства TCP/IP.

В ГЛОИС может быть добавлена поддержка любых дополнительных протоколов обмена данными, позволяющих подключить специализированные системы различных типов и различных производителей

1.4. Общие требования к организации подключения

В соответствии с нормативно-правовыми актами в сфере защиты информации в ГЛОИС приняты меры по защите информации:

1. Хранение и обработка информации, содержащейся в ГЛОИС, а также обмен информации осуществляются после принятия мер по защите указанной информации от повреждения или утраты, предусмотренных нормативно правовыми актами в области защиты информации.
2. Администраторы соответствующих уровней (администратор владельца, администратор клиента, администратор клиентского объекта) назначают лиц, ответственных за внесение сведений в ГЛОИС.
3. В соответствии с Законодательством, указанные лица (согласно п. 2) несут ответственность за полноту, достоверность и актуальность сведений, внесённых ими в ГЛОИС.

2. Технические требования

2.1 Требования к организации подключения

Организация подключения к ГЛОИС осуществляется в соответствии с требованиями:

- Условия договора на подключение;
- Настоящих технических условий.

2.1.1 Требования к протоколам обмена данными

На уровне клиентского объекта, для передачи данных между конечными устройствами и контроллерами передачи данных (КПД) используются протоколы связи клиентских технических систем, протоколы обмена данными, позволяющие подключить специализированные системы различных типов и различных производителей.

Взаимодействие между клиентским объектом, отдельными техническими системами (с одной стороны), и ГЛОИС (с другой стороны) осуществляется с использованием стека протоколов семейства TCP/IP по линиям связи сети Интернет. При этом ГЛОИС принимает передаваемую информацию от конечных устройств в формате работы контроллеров передачи данных (КПД).

Декодирование и нормализация параметров происходит на уровне ГЛОИС и не влияет на работу технических систем.

Схема подключения к ГЛОИС:

- При подключении к ГЛОИС требуется наличие статических IP-адресов сети у каждого из устройств передачи данных (ТД-точек доступа).
- В результате опроса ТД, данные передаются на IP-адрес облачного сервиса, где они подвергаются дальнейшей обработке.

По вопросам работы ГЛОИС – можно связаться с группой технической поддержки (support@glois.info).

2.1.2 Требования к линиям связи

Обеспечение подключения к сети Интернет (оплата) возлагается на пользователей ГЛОИС.

Для ГЛОИС могут использоваться: Ethernet, Wi-Fi, GPRS.

2.2 Требования к реализации защищённого взаимодействия

При построении системы информационной безопасности ГЛОИС учитывается полный перечень возможных угроз и путей, с использованием которых может быть нарушена работа ГЛОИС. Основные угрозы: несанкционированный доступ, действия вредоносного программного обеспечения и др.

В целях защиты информационных ресурсов ГЛОИС обеспечиваются и постоянно поддерживаются следующие мероприятия:

- конфиденциальность обрабатываемой и хранимой информации;
- целостность (достоверность) обрабатываемой и хранимой информации.

Программные средства информационной безопасности ГЛОИС обеспечивают:

- защиту от несанкционированного доступа;
- конфиденциальность данных;
- исключение воздействия вредоносного программного обеспечения («компьютерных вирусов», резидентов, отладчиков и т.д.);
- защиту от действий недобросовестного или недостаточно квалифицированного персонала.

Осуществление функционирования программно-технических мер информационной безопасности производится при обеспечении технических (физических) и организационных мер защиты.

Технические меры включают в себя:

- использование механизмов защиты активов от несанкционированного доступа (далее - НСД);
- использование штатных функций защиты информации и разграничений доступа ОС, СУБД и оборудования;
- использование дополнительных средств контроля целостности данных.

Организационные меры включают в себя:

- выполнение инструкций организации по обеспечению безопасности информации;
- выполнение инструкций по эксплуатации средств подсистемы информационной безопасности (далее - ПИБ);
- мероприятия по защите оборудования и ПО от несанкционированного доступа.

Программные средства защиты ГЛОИС от несанкционированного доступа обеспечивают выполнение функций:

- защита каналов передачи данных;
- аутентификация пользователей при входе в систему;
- аутентификация и авторизация пользователей при организации информационного обмена с программно-техническим комплексом ГЛОИС;

- аутентификация и авторизация пользователей при работе с компонентами системы;
- контроль прав доступа;
- управление доступом на всех этапах функционирования системы, в соответствии с политиками доступа для всех категорий обслуживающего персонала и пользователей;
- защиту ГЛОИС от несанкционированного изменения и доступа (ключей, параметров алгоритмов, настроек прав разграничения доступа, справочников, конфигурационных файлов и др.) программно-техническими, организационными методами;
- контроль обращения к ресурсам системы;
- регистрация попыток несанкционированного доступа к ресурсам;
- ведение журналов работы компонентов системы.

Требования по безопасности могут быть уточнены на этапе проектирования и подключения к системе (по согласованию сторон).

В ГЛОИС разработан регламент архивирования и резервного копирования штатными средствами системы, определено место хранения копий.

Для обеспечения конфиденциальности передаваемой информации в режиме доступа возможно использование дополнительных процедур шифрования, а для обеспечения юридической значимости, контроля целостности и подлинности информации – электронной цифровой подписи (ЭЦП). Возможность использования шифрования и электронной подписи требует уточнения у службы поддержки ГЛОИС.

Организационные (административные) меры требуют строгого соблюдение правил обращения со служебной информацией.

Функционирование клиентской части должно осуществляться в условиях строго регламентированного и контролируемого доступа.

Конкретные средства защиты программных компонентов и ключевой информации от НСД определяются на стадии подключения клиента к ГЛОИС.

2.3 Требования к программному обеспечению

Пользователи ГЛОИС должны использовать актуальные версии интернет-браузеров.


Windows


Unix


Mac OS