ОБЯЗАТЕЛЬНЫЕ СТАНДАРТНЫЕ ТРЕБОВАНИЯ

§1. Требования технических регламентов.

При проектировании и изготовлении оборудования должны быть учтены требования (По запросу Продавца, Покупатель предоставляет Продавцу все необходимые нормативные документы):

- Технические Регламенты Таможенного Союза:
  - ТР ТС 010/2011 «О безопасности машин и оборудования»;
  - ТР ТС 004/2011 «О безопасности низковольтного оборудования»;
  - ТР ТС 020/2011 «Электромагнитная совместимость технических средств»;
  - все прочие Технические Регламенты ТС, применимых для поставляемого оборудования.

- Пункты ФНиП "Обеспечение промышленной безопасности при организации работ на опасных производственных объектах горно-металлургической промышленности":
Устанавливаемые замки-выключатели должны соответствовать следующим требованиям:
  - иметь высокую степень защиты от случайного открытия похожим ключом;
  - ключ может быть изъят из замка-выключателя только в отключенном положении при разомкнутых контактах замка-выключателя.

- Пункты ФНиП "Правила безопасности процессов получения или применения металлов":
  - Все технические устройства, имеющие движущиеся части, которые могут являться источниками опасности травмирования работников или воздействия на другое оборудование, должны быть ограждены согласно требованиям проекта, нормативных правовых актов, требованиям изготовителей. Исключением являются движущиеся части, ограждение которых не допускается их функциональным назначением, а также движущиеся части, расположенные на высоте более 2,5 м и не представляющие опасности.
  - Зубчатые, ременные и цепные передачи независимо от высоты их расположения и скорости движения должны иметь сплошное ограждение.
  - Съемные ограждения должны быть снабжены устройствами, исключающими их случайное открытие или снятие, а при необходимости,

OBLIGATORY STANDARD REQUIREMENTS

§1. Technical regulations requirements.

During design and production of the Equipment the following requirements should be considered (at Seller's request Buyer provides Seller with all necessary regulations):

- Technical Regulations of the Customs Union:
  - TR CU 010/2011 "On safety of machines and equipment";
  - TR CU 004/2011 "On safety of low-voltage equipment";
  - TR CU 020/2011 "Electromagnetic compatibility of technical means";
  - all other Technical Regulations CU relevant for the delivered Equipment.

- Clauses of Federal Rules and Regulations "Industrial safety maintenance when arranging works on hazardous production facilities in mining and metallurgical industry":
Keylock-switches to be installed shall meet the following requirements:
  - have high protection level against accidental unclose with a similar key.
  - key can be withdrawn from the keylock-switch only in disengaged condition with open contacts of the keylock-switch.

- Clauses of Federal Rules and Regulations "Safety regulations for metals manufacturing and application":
  - All technical devices having moving parts which can be workers' traumatizing hazards or hazards of impact on other equipment, shall be guarded and fenced in accordance with the engineering design requirements, with laws and regulations, manufacturers' requirements. Exclusions are moving parts, for which their purpose of function makes their guarding or fencing impossible, as well as moving parts which are located at height of more than 2,5 m and which do not pose threat.
  - Gear, belt and chain drives regardless of their arrangement height and movement speed shall have removable closed sheeting (safety guards).
  - Removable safety guards shall be supplied with devices, excluding their accidental opening or demounting, and if necessary, have

иметь блокировки, обеспечивающие прекращение рабочего процесса при их снятии или открытии. Ограждения должны поставляться комплектно с техническими устройствами.

blockings, providing working process shutdown if they are demounted or opened. Safety guards shall be delivered together with technical devices.

§2.Требования по комплектации оборудования и программного обеспечения для системы автоматического управления.

§2. Requirements for hardware and software for automatic control system.

Система автоматического управления (САУ) построена на электрооборудовании фирмы Siemens. Основой САУ является программируемый логический контроллер (ПЛК) Simatic S7 фирмы Siemens. Распределенные блоки (подключаемые к контроллеру по промышленной сети) – фирмы Siemens.

Automatic control system is based on Siemens electrical equipment. The basis of the automatic control system is programmable logic controller (PLC) Simatic S7, Siemens. Distributed blocks (connected to the controller via industrial network) are Siemens.

САУ управляет приводами, обрабатывает сигналы с датчиков и т.д. и управляет вспомогательными механизмами. В САУ исключены специфические электронные блоки производства других производителей, которые управляют отдельными частями Оборудования.

Automatic control system controls drives, handles signals from sensors and etc., and operates the accessory mechanisms. There are no specific electronic modules manufactured by other producers, which operate the separate parts of the Equipment.

Панель оператора производства Siemens. Система визуализации так же разработана на базе программного обеспечения фирмы Siemens.

Operator panel is Siemens. Visualization system is also designed on the base of Siemens software.

При управлении электроприводом (частотными преобразователями) Оборудования по промышленной сети, электропривод выполнен на частотных преобразователях фирмы Siemens.

In case that the Equipment electric drive (frequency inverters) is controlled via industrial network, the electric drive is based on Siemens frequency inverters.

Энкодеры для электроприводов управляемых по промышленной сети производства Siemens.

Encoders for electric drives, controlled via industrial network, are Siemens.

Всё программное обеспечение САУ написано с использованием программных инструментальных средств фирмы Siemens: Step7, Protool, WinCC, WinCC flexible, Starter, TIA Portal.

All automatic control system software is coded using Siemens software tools: Step7, Protool, WinCC, WinCC flexible, Starter, TIA Portal.

Программы управления ПЛК и алгоритм их работы, системы визуализации, параметры преобразователей, инструкции по эксплуатации и наладке, пароли доступа должны быть переданы после полной отладки Покупателю.

PLC control programs and their operation algorithm, visualization systems, inverters parameters, operation and setup instructions, access passwords (keys) shall be transferred to Buyer after the Equipment set-up accomplishment.

§3. Требования по информационной безопасности

§3. Information security requirements

Требования данного раздела обязательны для выполнения Продавцом и/или Производителем Оборудования. Выполнение этих требований будет учитываться при приемке Оборудования.

The requirements of this section are compulsory for the Equipment Seller and/or Manufacturer. Fulfillment of these requirements will be taken into account when accepting the Equipment.

Невыполнение согласованных Продавцом и Покупателем требований информационной безопасности может
служить основанием для отказа в подписании Акта о вводе Оборудования в эксплуатацию и выходе на согласованную производительность с отметкой «без замечаний» .
По согласованию с Покупателем допускается внесение изменений в п.1 (Требования к Антивирусной защите), п.3 (Организация удаленного доступа к ресурсам), п.5 (Требования к организации мониторинга информационной безопасности), п.9 (Требования по организации беспроводной технологической ЛВС), п.10 (Требования к сетевому оборудованию и его конфигурированию) в соответствии с используемыми в системе типами оборудования. Остальные требования редактированию не подлежат.
При наличии в проекте Оборудования автоматизированных рабочих мест, серверов, любого сетевого оборудования, работы и материалы для подключения Оборудования к технологической сети включаются в проект Оборудования, если в Контракте или Приложении к нему не оговорено иное. В этом случае, все необходимые устройства и материалы включены в объем поставки Оборудования; обеспечение подключения осуществляется силами Покупателя. Подключение таких систем к технологической сети ***обязательно****.*

Failure to comply with the information security requirements agreed by the Seller and the Buyer may serve as a basis for refusing to sign the Protocol about the Equipment putting into operation and achievement of the agreed productivity with the note "accepted without any objections".
By agreement with the Buyer, amendments may be introduced to p.1 (Requirements to antivirus protection), p. 3 (Requirements to remote access to resources), p. 5 (Requirements to information security monitoring), p. 9 (Requirements to setting up of wireless process LAN), p. 10 (Requirements to network equipment and its configuration) in accordance with the types of equipment used in the system. The remaining requirements are not subject to any changes.

If there are workstations, servers, any network equipment in the Equipment configuration, works and materials for connecting the Equipment to the technological network should be included in the Equipment configuration, unless otherwise specified in the Contract or in an Appendix to the Contract. In this case, all the necessary devices and materials should be included in the scope of supply of the Equipment; the connection is provided by the Buyer. The connection of such systems to the corporate network is ***compulsory****.*

Перечень используемых сокращений:
- АВЗ – антивирусная защита;
- АРМ – автоматизированное рабочее место;
- ДМЗ – демилитаризованная зона;
- АСУТП – автоматизированная система управления технологическим процессом;
- КСПД – Корпоративные сети передачи данных;
- ПК – персональный компьютер;
- ПО – программное обеспечение;
- ЛВС – локальная вычислительная сеть;
- КИС – корпоративная информационная система);
- ТСПД – Технологическая сеть передачи данных

List of abbreviations:
- AVP – Antivirus Protection;
- WS – Workstation;
- DMZ – Demilitarized Zone;
- APCS – Automated Process Control System;
- CDTN – Corporate Data Transfer Networks;
- PC – Personal Computer;
- SW – Software;
- LAN – Local Area Network;
- CIS – Corporate Information System;
- PDTN – Process Data Transfer Networks

1. Требования к Антивирусной защите
(Применимо при наличии в системе АРМ и серверов)
На все внедряемые АРМ и сервера должны быть установлены предусмотренные стандартами группы компаний «Северсталь» средства антивирусной защиты, управляемые через централизованный сервер администрирования,

1. Requirements to antivirus protection
(Applicable if there are workstations and servers in the system)
Corporate antivirus tools, defined by the standards of the Severstal group of companies, controlled via centralized administration server located in demilitarized zone (DMZ) shall be

размещенный в демилитаризованной зоне (ДМЗ).
Запрещается подключать внедряемые АРМ и сервера в сеть без установленных средств АВЗ и актуальных обновлений безопасности

installed on all introduced workstations and servers.
It is forbidden to connect the new workstations and servers to the network without installed antivirus tools and latest safety updates.

2. Требования к обновлениям безопасности
На все программное обеспечение (операционные системы, прошивки контроллеров, сетевого оборудования и т.д.) – должны быть установлены последние обновления безопасности, которые закрывают известные уязвимости. В случае несовместимости с действующими системами, необходима разработка и реализация дополнительных мероприятий, согласованных с Управлением Информационной Безопасности Покупателя.

2. Requirements to security updates
The latest security updates that eliminate known vulnerabilities shall be installed on all software (operating systems, firmware of controllers, network equipment). In case of incompatibility with existing systems, development and implementation of additional measures shall be required as agreed with the Information Security Department and the Automation Department.

3. Организация удаленного доступа к ресурсам
(Применимо при необходимости организации удаленного доступа в момент наладки и гарантийного сопровождения, обратить внимание на ограничения)
Организация удаленного доступа к ресурсам АСУТП должна осуществляться посредством шлюзов терминалов, расположенных в ДМЗ.
Работа пользователей из КСПД с ресурсами АСУТП осуществляется путем подключения на терминальный сервер в ДМЗ.
Все пограничные сервисы, осуществляющие взаимодействие технологической сети и КСПД для сопровождения АСУТП, должны быть перенесены в организованную ДМЗ.
Запрещена маршрутизация трафика на хостах в ДМЗ (сквозное прохождение трафика через ДМЗ).
Запрещена организация удаленного доступа к ресурсам АСУТП через открытые каналы связи (3G, 4G/LTE).
Запрещена установка средств удаленного администрирования (TeamViewer и т.д.).
Все решения по организации удаленного доступа согласовываются с Управлением Информационной Безопасности Покупателя.

3. Requirements to remote access to resources
(Applicable if it is necessary to organize remote access during commissioning and warranty support works, special attention shall be paid to the limitations)
Remote access to APCS resources shall be granted via terminals gateways located in DMZ.

The work of users from the CDTN with the resources of the APCS should be performed by connecting to the terminal server in the DMZ.
All border services that interact with the technological network and CDTN to support APCS should be transferred to the organized DMZ.
It is prohibited to route traffic on hosts in the DMZ (end-to-end traffic through the DMZ).

Granting of remote access to APCS resources via open communication channels (3G, 4G/LTE) is prohibited.
Installation of remote administration tools (TeamViewer, etc.) is prohibited.
All remote access-related solutions shall be agreed upon with the Buyer's Information Security Department.

4. Требования по подключению оборудования сотрудников сторонних организаций (Продавца и/или Производителя)
При необходимости подключения сотрудников Продавца и/или Производвителя к контроллерам, серверам, рабочим станциям АСУТП с собственных ноутбуков во время наладки необходимо обеспечить:
- Наличие средств АВЗ с актуальными базами;

4. Requirements to connection of the equipment of external organizations' employees (Seller's and/or Manufacturer's)
When Seller's and/or Manufacturer's employees need to connect their laptop computers to APCS controllers, servers or workstations during commissioning, the following shall be ensured:

- Availability of antivirus protection software with updated virus bases;

- Полную проверку ПК средствами АВЗ;

- Наличие установленных критичных обновлений безопасности операционной системы.

- Full virus checking by antivirus protection software;
- Installation of all critical security updates for the operating system.

5. Требования к организации мониторинга информационной безопасности
(Применимо при развертывании больших информационных систем)
С целью мониторинга информационной безопасности предусмотреть:
- Порты конфигурирования сетевого оборудования выделить в отдельный сегмент (VLAN);
- Для аутентификации на сетевом оборудовании использовать протокол TACACS+ и централизованные учетные записи;
- Настроить сбор событий (со всех серверов, рабочих станций, активного сетевого оборудования, внедренных в рамках проекта) и пересылку по протоколу syslog на сервер сбора событий производства;

- Обеспечить программный контроль изменения конфигураций всего установленного в рамках проекта активного сетевого оборудования;
- Комплекс технических и программных средств должен гарантировать целостность(неизменяемость) обступаемых и обрабатываемых данных;
На всех АРМ и Серверах должны быть настроены политики безопасности и установлены агенты системы мониторинга информационной безопасности. Настраивается вывод событий (уровень событий согласовывается с Управлением Информационной Безопасности Покупателя) по протоколу syslog на сервер сбора событий производства (ip адрес предоставляет Управление Информационной Безопасности Покупателя).

5. Requirements to information security monitoring
(Applicable when deploying large information systems)
The following shall be provided for monitoring of information security:
- The ports for configuring of network equipment shall be arranged as a separate segment (VLAN);

- TACACS+ protocol and centralized accounts shall be used for authentication on network equipment;
- Acquisition and forwarding of events (from all servers, workstations, active network equipment introduced within the framework of the project) shall be set up using the syslog protocol to the events acquisition server of the production facility;
- Software check of configuration changes for all active network equipment installed within the framework of the project shall be ensured;
- The package of hardware and software shall ensure integrity (immutability) of the processed and related data;

Security policies shall be set up and agents of the information security monitoring system shall be installed on all introduced workstations and servers. Forwarding of events (the event level to be agreed with the Information Security Department) shall be set up using the syslog protocol to the events acquisition server of the production facility (IP-address to be provided by the Information Security Department);

6. Требования к срокам и условиям хранения данных в информационной системе
Резервное копирование ПО системы управления и диагностики необходимо осуществлять при передаче системы в эксплуатацию и при каждом изменении ПО в течении гарантийного срока обслуживания.
Хранение резервных копий ПО предусмотреть не менее чем на трёх носителях, расположенных в разных помещениях, исключающих доступ посторонних лиц. Каждый носитель должен иметь маркировку, включающую в себя наименования агрегата, либо системы управлениям, на которой применяется ПО.

6. Requirements to the conditions and period of data storage in the information system
The control and diagnostic system software should be backed up when the system is put into operation and every time the SW is changed during the warranty period.

SW back-up copies shall be reproduced on at least three carriers located in different rooms with no access for third party persons. Each data carrier shall bear marking including the name of production unit or control system using the software.

7. Требования к аудиту событий в управляющей системе

Необходимо вести аудит событий входа/выхода пользователя в систему. Журнал аудита должен быть недоступен для редактирования ни одному из пользователей и храниться не менее 6 месяцев.

7. Requirements to audit of events in control system

User login/logout events shall be audited The audit log shall be unavailable for editing to any of the users and shall be stored during at least 6 months.

8. Требования к разграничению доступа к информации в системе

Для каждого пользователя должны быть заведены уникальные учётные записи, за исключением особых случаев, связанных с выполнением функциональных обязанностей группой работников с одним приложением. Список работников, использующих групповые учётные записи, должен быть строго определён. Групповые учётные записи могут быть созданы только для операторов (иных работников технологического персонала), управляющих агрегатом (Оборудованием) или его узлами.

8. Requirements to differentiation of access privileges to information in the system

A unique account shall be assigned to each user with exception of special cases when a group of employees have to work with the same application as part of their functional duties. The list of employees using group accounts shall be well-defined. Group accounts may be created only for operators (or other process personnel) controlling the equipment or its units.

9. Требования по организации беспроводной технологической ЛВС

(Применимо при использовании данной технологии)

- беспроводная сеть должны быть выделена в отдельный сегмент и относиться к технологическим сетям;
- беспроводная сеть должна быть отделена от проводных технологических ЛВС аппаратными маршрутизаторами с ACL;
- беспроводная сеть должна быть физически изолирована от информационной сети (КИС);
- беспроводной сети должно быть присвоено уникальное имя (SSID);
- на оборудовании беспроводной сети должна быть отключена рассылка широковещательных фреймов «beacon»;
- зона покрытия не должна превышать рабочую зону;
- для защиты трафика должен использоваться стандарт WPA2 с протоколом EAP-TLS;
- для аутентификации должен использоваться протокол 802.1 x и сервер аутентификации (контроллер для управления беспроводной инфраструктурой). При невозможности подключения WI-FI точки к контроллеру управления и использования RADIUS сервера необходимо применять метод сертификации беспроводных устройств WPA-2 Personal с использованием статического ключа PSK (Pre-Shared Key). При этом должен быть разработан и согласован с Управлением Информационной Безопасности Покупателя регламент смены

9. Requirements to setting up of wireless process LAN

(Applicable when using this technology)

- the wireless network shall be detached into a separate segment and shall belong to process networks;
- the wireless network shall be separated from wired process LANs by hardware routers with ACL;
- the wireless network shall be physically isolated from the information network (CIS);
- wireless network shall have a unique name assigned (SSID);
- "beacon" frame broadcasting shall be switched off on the wireless network equipment;
- the signal level in the work area shall not exceed the working area;
- traffic shall be protected via WPA2 with the EAP-TLS protocol;
- 802.1X protocol, as well as the authentication server (wireless infrastructure controller) shall be used for authentication purposes. If it is impossible to connect a WI-FI point to the control controller and use a RADIUS server, then WPA-2 Personal wireless device certification method using a static PSK (Pre-Shared Key) shall be used. At the same time, the key change regulations shall be developed and agreed with the Buyer's Information Security Department; in addition, MAC address based filtering of client requests shall be applied to the access points. A list of

ключа, дополнительно на точках доступа должна быть применена фильтрация запросов клиента на основе MAC-адреса. На каждой точке создается список разрешенных MAC-адресов;

allowed MAC addresses shall be created for each point;

- на кранах устанавливается только клиентское беспроводное оборудование.

- only client wireless equipment shall be installed on cranes.

10. Требования к сетевому оборудованию и его конфигурированию

*(Применимо при использовании в проекте **нового** сетевого оборудования)*

Запрещено использовать в ТСПД неуправляемое сетевое оборудование.

Обязательно включить блокировку всех неиспользуемых портов на сетевом оборудовании.

10. Requirements to network equipment and its configuration

*(Applicable when using **new** network equipment in the project)*

Uncontrolled network equipment shall not be used in Process Data Transfer Networks (PDTN).

Blocking of all unused ports on network equipment shall be provided.

11. Требования к разрабатываемому программному обеспечению

Перед внедрением в промышленное использование программного обеспечения, разработанного силами Производителя Оборудования, необходима передача исходного кода для проведения анализа на наличие уязвимостей. Ввод системы в эксплуатацию до устранения уязвимостей невозможен.

11. Requirements to the developed software

Prior to starting the industrial use of the software developed by the Equipment Manufacturer, the source code shall be provided for vulnerability analysis. The system cannot be put into operation until the vulnerabilities are eliminated.