

УТВЕРЖДАЮ

Начальник службы автоматизации

ООО «НПП ОЗНА-Инжиниринг»

\_\_\_\_\_\_\_\_\_\_В.О. Литвинов

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**Система измерений количества и**

**показателей качества нефти**

**№102 ПСП «Тайшет-2»**

**ООО «Транснефть - Восток»**

ОИ 410-01.00.00.00.000 И3

**Руководство куратора информационной безопасности**

РАЗРАБОТАЛ

Главный специалист по РПО МСО

ООО «НПП ОЗНА-Инжиниринг»

\_\_\_\_\_\_\_\_\_\_\_А.С. Русских

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Уфа 2020

# Содержание

[Содержание 2](#_Toc31964218)

[Введение 3](#_Toc31964219)

[1 Обозначения и сокращения 4](#_Toc31964220)

[2 Назначение и условия выполнения программы 5](#_Toc31964221)

[3 Выполнение программы и сообщения оператору 7](#_Toc31964222)

[3.1 Запуск программы 7](#_Toc31964223)

[3.2 Приёмы работы 7](#_Toc31964224)

[3.3 Техника безопасности 7](#_Toc31964225)

[4 Интерфейс АРМ 8](#_Toc31964226)

[5 Получение доступа к функциям АРМ 9](#_Toc31964227)

[5.1 Регистрация в ОС 9](#_Toc31964228)

[5.2 Регистрация в системе отображения 9](#_Toc31964229)

[5.3 Смена пароля пользователем 10](#_Toc31964230)

[6 Подключения к сетевым устройствам 11](#_Toc31964231)

[6.1 Подключение к ПЛК 11](#_Toc31964232)

[6.2 Подключение к ИВК 11](#_Toc31964233)

[6.3 Подключение к коммутаторам 12](#_Toc31964234)

[7 Просмотр журналов 13](#_Toc31964235)

[7.1 Просмотр журналов АРМ-оператора 13](#_Toc31964236)

[7.2 Просмотр журналов ИВК 13](#_Toc31964237)

[7.3 Просмотр журналов коммутаторов 14](#_Toc31964238)

[8 Проверка информационной безопасности 16](#_Toc31964239)

[8.1 Проверка настройки средств защиты информации 16](#_Toc31964240)

[8.2 Проверка установленных обновлений 16](#_Toc31964241)

[8.3 Проверка перечня установленного ПО АРМ 16](#_Toc31964242)

[8.4 Проверка целостности ППО АРМ 16](#_Toc31964243)

[Лист регистрации изменений 18](#_Toc31964244)

# Введение

Настоящее руководство предназначено для персонала, осуществляющих контроль обеспечения информационной безопасности (далее по тексту – Куратор ИБ) на АРМ оператора.

В руководстве содержатся:

1. сведения, необходимые для доступа к операционной системе (ОС);
2. сведения, необходимые для проверки состояния средств обеспечения информационной безопасности, реализованных в АРМ;
3. сведения, необходимые для диагностики и чтения журналов с сетевого оборудования.

# Обозначения и сокращения

В настоящем документе применены следующие обозначения и сокращения:

|  |  |
| --- | --- |
| **АСУТП** | автоматизированная система управления технологическим процессом |
| **СА** | система автоматизации |
| **ПК** | программный комплекс |
| **ОС** | операционная система |
| **ПК** | персональный компьютер |
| **ПО** | программное обеспечение |
| **ППО** | прикладное программное обеспечение |
| **СПО** | системное программное обеспечение |
| **СОИ** | система обработки информации |
| **СИКН** | система измерения количества и показателей качества нефти |
| **ПЛК** | программируемый логический контроллер |
| **ИВК** | измерительно-вычислительный комплекс (контроллер) |
| **АРМ** | автоматизированное рабочее место |
| **SCADA** | Supervisory Control And Data Acquisition (диспетчерское управление и сбор данных) |

# Назначение и условия выполнения программы

ПО АРМ предназначено для:

1. наглядного представления состояния средств измерений, исполнительных механизмов и технологического процесса в целом;
2. формирования архивного журнала событий;
3. формирования архива трендов измеряемых параметров;
4. оповещения оператора об отклонениях технологического процесса от заданного режима работы и обнаруженных диагностируемых неисправностях оборудования;
5. управления исполнительными механизмами;
6. конфигурирования технологических алгоритмов;
7. обеспечения информационной безопасности СА.

Для корректной работы ПО АРМ необходимо выполнение следующих условий:

1. ПО установлено и настроено в соответствии с указаниями, приведёнными в документе «Руководство программиста. Часть 2. Руководство по инсталляции ПО» и «Руководство администратора»;
2. состав аппаратных средств АРМ соответствует указанным в спецификациях на СА;
3. ПО, установленное и настроенное в ПЛК СА и ИВК СА, совместимо с ПО, установленным в АРМ;
4. не нарушены условия эксплуатации оборудования АРМ, ПЛК и ИВК (сбои питания, попадание посторонних предметов внутрь корпусов устройств, нарушения климатических показателей и др.);
5. обеспечена защита от несанкционированных вмешательств в ПО ПЛК, ИВК и АРМ;
6. Куратор ИБ должен иметь полное представление о структуре СА, знать способы обеспечения информационной безопасности СА, установленные в организации, уверенно владеть навыками работы с ЭВМ в объёме должностных обязанностей.

Для контроля технологического процесса предусмотрены три АРМ-оператора, отображающие устройства которые выполнены в виде настольного монитора, а устройства ввода представляют собой настольные клавиатуру и манипулятор «мышь» (далее по тексту - мышь), расположенные на столе оператора.

Каждый АРМ работает непрерывно и независимо. ПО, установленное в каждом АРМ, идентично.

Программный комплекс для АРМ Оператора СИКН предполагает работу с контроллерами потока Floboss S600/Floboss S600+ и программируемыми логическими контролерами S7-400H, используемыми в составе системы измерения количества и показателей качества нефти, в режиме двустороннего обмена данными.

# Выполнение программы и сообщения оператору

## Запуск программы

В штатном режиме работы ПО АРМ запущено и готово для проверки состояния средств защиты информации.

При необходимости включения/выключения, перезагрузки ПО АРМ, а также доступа к функциям конфигурирования ПО следует обратиться к обслуживающему персоналу или к персоналу, осуществляющему сопровождение ПО АРМ.

## Приёмы работы

При работе с АРМ используются типовые операции, выполняемые с помощью клавиатуры и мыши.

Типовые операции, применяемые при работе с АРМ («открыть окно», «ввести число», «подать команду» и др.) приведены в документе «Руководство оператора».

## Техника безопасности

При работе с АРМ запрещается:

1. работать на заведомо неисправном оборудовании;
2. эксплуатировать АРМ без знания и применения безопасных способов работы и обращения с ЭВМ, знания мест расположения первичных средств пожаротушения и правил пользования ими, способов оказания первой (доврачебной) помощи;
3. изменять настройки и код ПО без участия квалифицированных специалистов, осуществляющих сопровождение ПО или разработчиков ПО, допущенных к работе с АРМ.

# Интерфейс АРМ

Описание интерфейса АРМ, а также способов работы с ним приведено в документе «Руководство оператора».

В руководстве оператора приведены:

1. приёмы работы с ПО АРМ;
2. описание графических элементов интерфейса АРМ;
3. описание процедур контроля технологического процесса средствами АРМ, в том числе:

- описание работы с журналами технологических событий и аварий (включая события с учётными данными пользователей АРМ);

- описание работы с трендами измеряемых параметров;

- описание способов контроля технологического оборудования и измеряемых параметров посредством подачи команд, ввода уставок и назначения режимов (для пользователей различного уровня доступа);

- описание способов настройки технологических алгоритмов (для пользователей различного уровня доступа);

1. сведения по диагностике СА, в том числе:

- сведения по диагностике оборудования СА;

- сведения по проверке технологических алгоритмов (посредством включения режимов имитации);

- сведения по контролю целостности ПО СА;

1. рекомендации по действиям персонала в нештатных ситуациях (связанных с работой ПО АРМ);
2. другие сведения, необходимые для работы с АРМ оператора.

# Получение доступа к функциям АРМ

## Регистрация в ОС

Для доступа к функциям ОС требуется:

1. зарегистрироваться в системе отображения под соответствующей учётной записью, получив доступ к ОС с правами доступа «Оператор» (как описано ниже);
2. в ОС с помощью меню «Пуск» (вызывается нажатием на клавиатуре клавиши «Windows») кликнуть ЛКМ на символе  и в раскрывшемся списке выбрать требуемую учётную запись («Куратор ИБ»);
3. получить доступ к ОС с правами доступа «Куратор ИБ», зарегистрировавшись под соответствующей учётной записью в окне блокировки Windows;
4. по окончанию работы в ОС с помощью меню «Пуск» (вызывается нажатием на клавиатуре клавиши «Windows») кликнуть ЛКМ на символе  и в раскрывшемся списке выбрать пункт «Выход»;
5. проконтролировать появление окна блокировки Windows на экране.

Заведенные и используемые в ОС учетные записи (в том числе технологические) представлены в документе «Руководстве администратора» в таблице 2.3.1.

## Регистрация в системе отображения

Работа Куратора ИБ с АРМ возможна при наличии соответствующей учётной записи в ПО. В отсутствии такой учётной записи следует обратиться к персоналу с уровнем доступа к АРМ «Администратор».

Сведения, необходимые для регистрации пользователя в системе приведены в документе «Руководство оператора». Сведения по уровням доступов с ППО представлены в документе «Руководство администратора» в таблице 2.18.1.

## Смена пароля пользователем

В случае подозрения на компрометацию пароля, а также в случае необходимости соблюдения равенства паролей на различных АРМ пользователь может самостоятельно изменить свой пароль.

Сведения, необходимые для смены пароля пользователя в системе приведены в документе «Руководство оператора».

# Подключения к сетевым устройствам

## Подключение к ПЛК

ПЛК СОИ СИКН выполнен на базе контроллера S7-400H производства Siemens. Для разработки ПО и диагностики контроллеров данной серии используется программный пакет «STEP 7».

Инструкция по подключению к ПЛК описана в документе «Руководство программиста. Часть 5. Руководство программиста среднего уровня».

Инструкция по установке и конфигурированию взаимодействия АРМ-оператора с ПЛК описана в документе «Руководство программиста. Часть 2. Руководство по инсталляции ПО» в п.3.6, п.4.3, п.4.4.

## Подключение к ИВК

ИВК СОИ СИКН выполнен на базе контроллеров Floboss S600 и Floboss S600+. Для разработки ПО контроллеров данных серий используются ПК «Config 600».

Инструкция по установке и конфигурированию взаимодействия АРМ-оператора с ИВК описана в документе «Руководство программиста. Часть 2. Руководство по инсталляции ПО» в п.3.4 и п.4.2.

Для диагностирования и просмотра журнала работы ИВК используется доступ к контроллеру через встроенный WEB-сервер. WEB -интерфейс ИВК, обеспечивает доступ к экранным данным, отчетам, операциям и диагностике через сеть. Число элементов, доступное для просмотра и/или редактирования, зависит от применяемого уровня доступа (см. документ «Руководство администратора» п. 2.17.

Для обеспечения доступа и функциональности в полном объеме рекомендуется использовать Windows® Internet Explorer® версии 6.0 или выше, хотя возможно использование и альтернативных web-браузеров.

WEB-интерфейс контроллера поддерживает до 5 параллельных сеансов одновременно, при этом управление возможно только из одного.

Доступ к контроллеру с помощью web-браузера:

* + - 1. Подключитесь к контроллеру с помощью сетевого порта.
      2. Если ПК уже подключен к локальной сети, откройте web-браузер.
      3. Введите в адресную строку браузера IP-адрес контроллера (в формате <http://nnn.nnn.nnn.nnn>) и нажмите «Enter» (IP-адрес указан в документе «Карта сетевых настроек компьютерного оборудования»).

Доступ к контроллеру с помощью ППО «ОЗНА-Flow» описан в документе «Руководство оператора» в п.14.

## Подключение к коммутаторам

В качестве коммутаторов СОИ СИКН используются коммутаторы Siemens SCALANCE X208.

Настройка и диагностика работы коммутаторов выполняется с помощью встроенного web-сервера. Для подключения необходимо выполнить следующие действия:

* + - 1. Подключитесь к коммутатору с помощью сетевого порта.
      2. Если ПК уже подключен к локальной сети, откройте web-браузер.

Введите в адресную строку браузера IP-адрес коммутатора (в формате <http://nnn.nnn.nnn.nnn>) и нажмите «Enter» (IP-адрес указан в документе «Карта сетевых настроек компьютерного оборудования»).

# Просмотр журналов

## Просмотр журналов АРМ-оператора

Инструкция по просмотру журналов ОС и ППО на АРМ-оператора указан в документе «Руководство по техническому обслуживанию» в п. 11.

## Просмотр журналов ИВК

Для просмотра журналов аварий и событий необходимо подключиться к web-серверу ИВК, согласно п.6.2, и авторизоваться в системе с соответствующими доступами.

Для просмотра журнала текущих аварий необходимо перейти в меню «Alarm» расположенную на верхней панели меню. Отобразится окно со списком исторических аварийных сигналов отображенное на рисунке 7.2.1.

Для просмотра журнала исторических аварий необходимо перейти в меню «Reports» расположенную на верхней панели меню и выбрать в правой панели меню «Alarm Archive». Отобразится окно со списком исторических аварийных сигналов отображенное на рисунке 7.2.2.

Для просмотра журнала исторических аварий необходимо перейти в меню «Reports» расположенную на верхней панели меню и выбрать в правой панели меню «Event Archive». Для сохранения отображаемого списка аварий на компьютер в текстовый файл (CSV) необходимо нажать кнопку «CSV», расположенную в правом верхнем углу окна.



Рисунок 7.2.1 – Окно «Alarm»

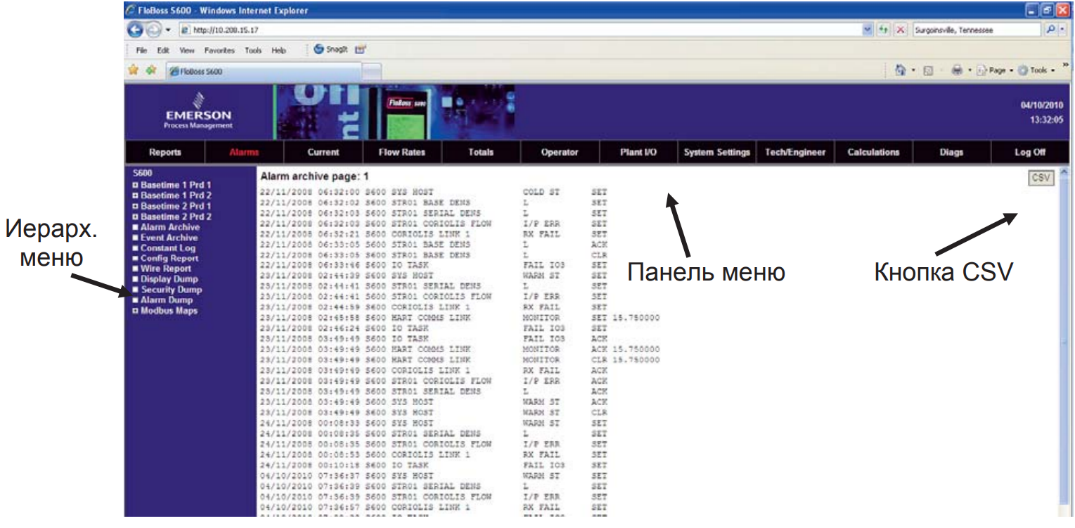


Рисунок 7.2.2 – Окно «Alarm Archive»

## Просмотр журналов коммутаторов

Для просмотра журналов коммутаторов событий необходимо подключиться к его web-сервер, согласно п.6.3, и авторизоваться в системе с соответствующими доступами.

Для чтения журнала событий коммутаторов Siemens SCALANCE X208 необходимо перейти в меню: «System» -> «Event Log» (см. рисунок 7.3.1). Для обновления списка событий нажмите кнопку «Refresh», для очистки списка событий необходимо нажмать кнопку «Clear Log».

Для сохранения всех событий в файл и загрузки его на компьютер нажмите кнопку «Save» в окне «Save & Load HTTP» (см. рисунок 7.3.2).

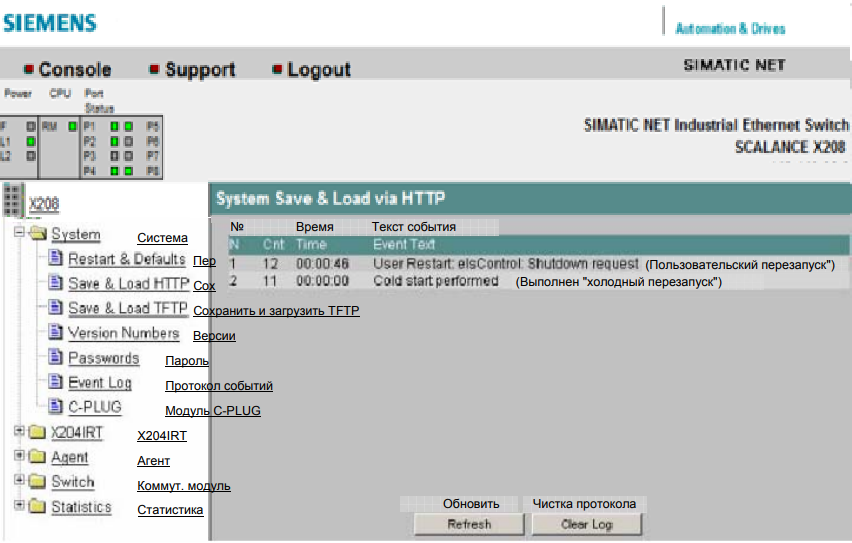


Рисунок 7.3.1 – Окно «Event Log»

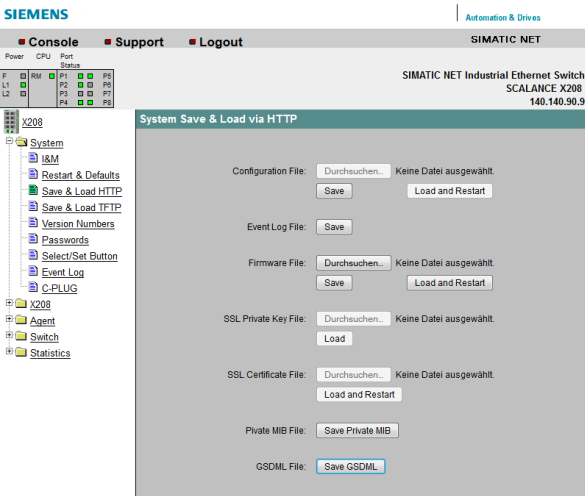


Рисунок 7.3.2 – Окно «Save & Load HTTP»

# Проверка информационной безопасности

## Проверка настройки средств защиты информации

Для проверки настройки средств защиты, реализованных в ПО АРМ необходимо войти в ОС под учётной записью пользователя «Администратор ОС» или «Куратор ИБ».

Сведения об используемых в ОС средствах защиты информации, а также сведения по настройкам этих средств приведены в документе «Руководство администратора».

При проверке не допускается включать дополнительные средства защиты информации, а также применять настраивать используемые средства без согласования с разработчиком ПО АРМ или персоналом, сопровождающим ПО СА.

## Проверка установленных обновлений

Проверка установленных в ОС обновлений проводится с применением штатных средств Windows. Сведения, необходимые для проверки установленных обновлений и наличия уязвимостей ОС приведены в документе «Руководство администратора».

## Проверка перечня установленного ПО АРМ

Проверка перечня установленного на АРМ ПО проводится с применением штатных средств Windows.

Проверка осуществляется сличением информации об установленном ПО, отображаемой на экране АРМ (средствами ОС), с перечнем, приведённым в документе «Спецификация ПО».

## Проверка целостности ППО АРМ

Проверка целостности ППО АРМ проводится с применением ПК «ОЗНА-Flow».

Проверка осуществляется сличением информации эталонных цифровых идентификаторов ППО с идентификаторами вычисленными на момент проверки. Сведения, необходимые для проверки приведены в документе «Руководство оператора» в п.21.

# Лист регистрации изменений

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Изм. | Номера листов | | | | Всего листов в документе | № документа | Подпись | Дата |
| Измененных | Замененных | Новых | Аннулированных |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |  |  |
| 16 |  |  |  |  |  |  |  |  |
| 17 |  |  |  |  |  |  |  |  |
| 18 |  |  |  |  |  |  |  |  |
| 19 |  |  |  |  |  |  |  |  |
| 20 |  |  |  |  |  |  |  |  |
| 21 |  |  |  |  |  |  |  |  |
| 22 |  |  |  |  |  |  |  |  |
| 23 |  |  |  |  |  |  |  |  |
| 24 |  |  |  |  |  |  |  |  |
| 25 |  |  |  |  |  |  |  |  |
| 26 |  |  |  |  |  |  |  |  |
| 27 |  |  |  |  |  |  |  |  |
| 28 |  |  |  |  |  |  |  |  |
| 29 |  |  |  |  |  |  |  |  |
| 30 |  |  |  |  |  |  |  |  |
| 31 |  |  |  |  |  |  |  |  |
| 32 |  |  |  |  |  |  |  |  |
| 33 |  |  |  |  |  |  |  |  |
| 34 |  |  |  |  |  |  |  |  |