ТЕКОН-АВТОМАТИКА
системы управления, диспетчеризации и учёта

ООО НПО "Текон-Автоматика"
Тел.: (495) 642-71-90, 971-41-21
Тел.: (499) 720-82-27 Факс: (499) 720-83-98
E-mail: tekon@tekon.ru Web: www.tekon.ru

ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ АСУД-248

Приводятся рекомендации по повышению надежности функционирования системы АСУД-248 при передаче данных между компонентами системы по компьютерным каналам связи.

Значительное развитие и распространение компьютерных сетей в последние годы делает их весьма привлекательными для использования в сфере решения задач диспетчеризации.

Для возможности использования сетевой инфраструктуры в качестве среды передачи диспетчерской информации в системе АСУД-248, были разработаны контроллеры инженерного оборудования (КИО), IP-концентраторы, модернизировано программное обеспечение.

Компьютерные сети можно разделить на публичные и частные.

Частная сеть (изолированная сеть) – представляет собой распределенную структуру, закрытую (защищенную) от доступа извне. Другими словами в частной сети находится только доверенное оборудование и доступ к ней (сети) имеют только доверенные пользователи. Примером такой частной сети, может служить локальная сеть предприятия или локальная офисная сеть (без выхода в сеть Интернет).

Публичная сеть – это сеть общего пользования. Основные отличия ее от частной в том, что к данной сети может быть подключено большое количество недоверенных («случайных») пользователей, и сеть не направлена на решение какой-то узкоспециализированной задачи. Наиболее яркий пример публичной сети – глобальная сеть Интернет.

С точки зрения функционирования диспетчерской системы, желательно чтобы среда передачи данных представляла собой именно частную сеть, а еще лучше – частную сеть, построенную специально и только для решения задач диспетчеризации. Что предотвратит возможный несанкционированный доступ к диспетчерскому оборудованию, возможные атаки на оборудование, связанные с отказом в обслуживании, со стороны других пользователей сети,

а также инфицирование оборудования диспетчеризации компьютерными вирусами, распространяемыми по сети.

В тоже время следует отметить, что частная сеть – это не обязательно сеть, не имеющая физического доступа к глобальной публичной сети. Условно говоря, частная сеть может быть реализована программно-техническими средствами провайдера сети путем «сокрытия и объединения» отдельных участков его публичной сети в частную сеть. При этом физически используются общие кабельные (проводные или беспроводные) линии провайдера, но обычные пользователи сети не имеют возможности доступа к диспетчерскому оборудованию, размещенному в такой частной сети. Выполняя монтаж новой диспетчерской, следует ориентироваться на данный вариант использования компьютерной сети.

Однако, на практике, компоненты диспетчерской системы зачастую располагаются именно в публичных сетях. При этом вопросу несанкционированного доступа к оборудованию не уделяется должного внимания: используются пароли по умолчанию, не применяется ограничение доступа к устройствам и т.п.

В связи с этим, далее будут приведены рекомендации повышающие безопасность функционирования системы АСУД-248, направленные на устранение возможного несанкционированного доступа к оборудованию. Пункты, отмеченные звездочкой (*), рекомендуется выполнять только опытным пользователям.

ПК ДИСПЕТЧЕРА

Рассматриваются ПК, предустановленные в Текон-Автоматика, но рекомендации в целом равнозначны и для других ПК.

На ПК установлены:

- операционная система (ОС) Windows XP Embedded;
- программа удаленного доступа VNC.

1. *Изменение паролей пользователей операционной системы.*

Для предотвращения доступа к ПК настоятельно рекомендуется выполнить изменение паролей для пользователей ОС.

По умолчанию в ОС зарегистрированы 3 пользователя:

Группа *«Администраторы»*:

- *Administrator* – служебный пользователь используется ремонтной службой Текон-Автоматика. Пароль не разглашается. Менять не следует!
- *AdminScada* – пользователь для выполнения настройки ПК и программного обеспечения. Пароль 0000.

Группа *«Продвинутые пользователи»:*

- *Dispatcher* – пользователь для работы диспетчера. Пароль 0000.

Следует изменить пароли для пользователей *AdminScada*, *Dispatcher*.

Для этого зайти в систему под пользователем *AdminScada*.

Выбрать *«Пуск / Панель управления / Администрирование / Управление компьютером»*.

В открывшемся окне, представленном на рисунке 1, последовательно выбрать пользователей *Dispatcher*, *AdminScada*, нажать правой кнопкой мыши и выбрать *«Задать пароль ...»*, подтвердить выполнение изменения пароля и в окне, представленном на рисунке 2, ввести новый пароль и нажать «*Ок*».

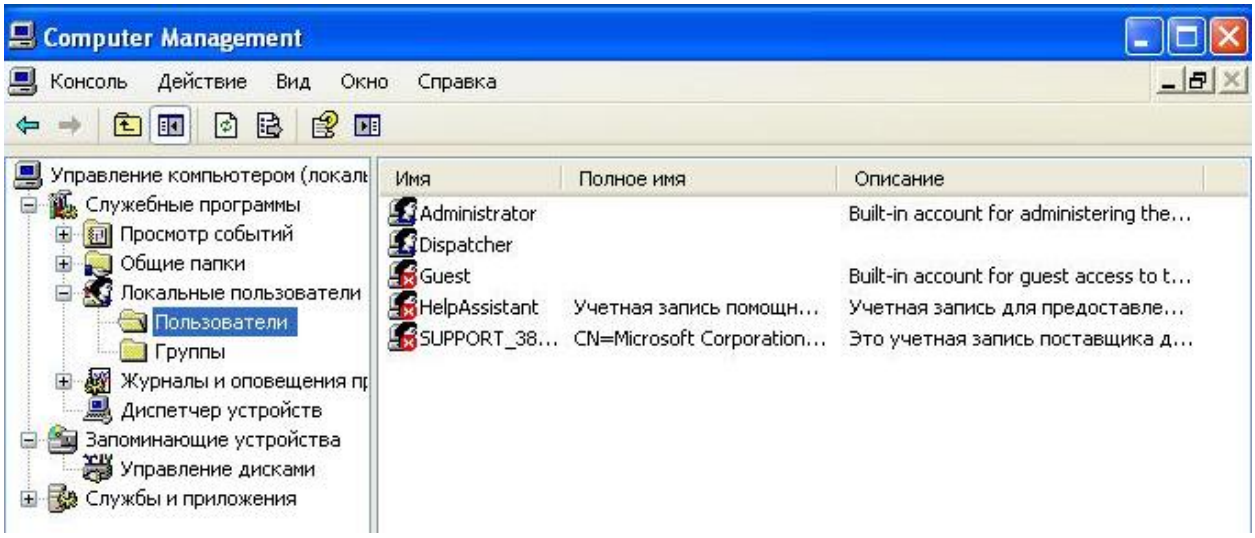

Рисунок 1 – Настройка учетных записей Windows.

Рекомендации по выбору пароля: не менее 6 символов, чередование букв и цифр.

Желательны разные пароли для *Dispatcher*, *AdminScada*.

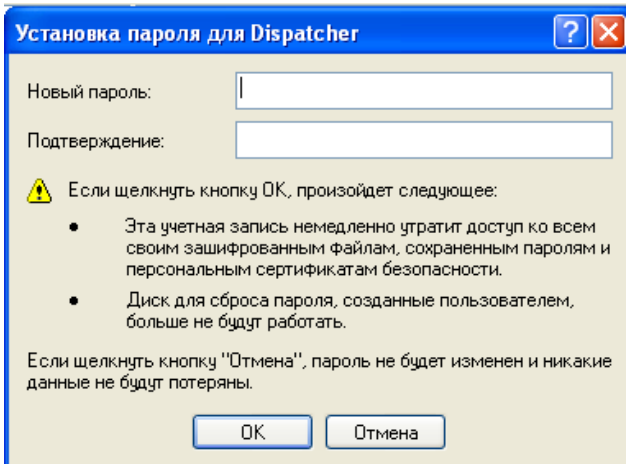

Рисунок 2 – Изменение пароля пользователя Windows.

Также следует убедиться, что в системе отключены другие учетные записи (см. рисунок 1). В противном случае, следует выбрать учетную запись, нажать правую кнопку мыши и в открывшемся окне, представленном на рисунке 3, установить флажок *«Отключить учетную запись»*.

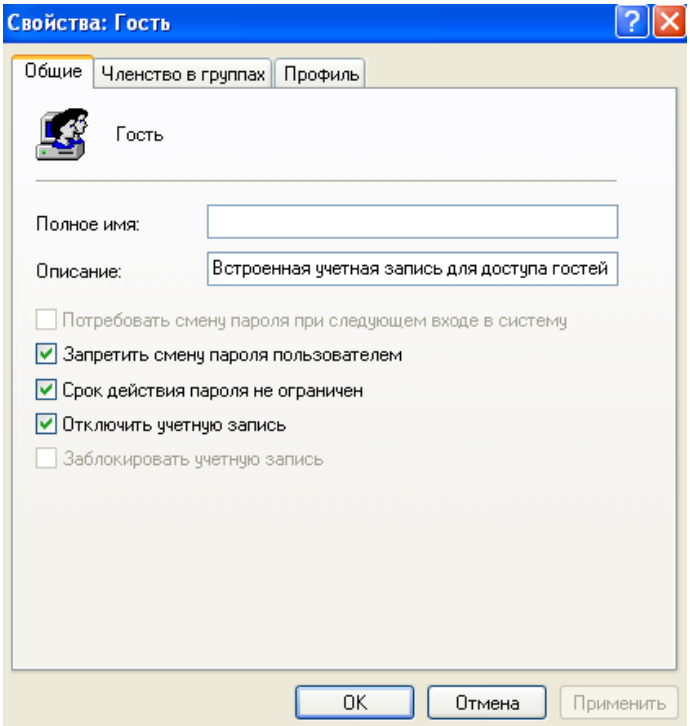

Рисунок 3 – Отключение записи пользователя Windows.

Если ПК диспетчера автоматически загружался после включения (без требования ввода пароля), то после изменения пароля пользователя *Dispatcher* необходимо изменить настройки загрузки операционной системы. Для этого выбрать *«Пуск / Выполнить»*, набрать *«control userpasswords2»*, нажать *«Выполнить»*. В открывшемся окне (рисунок 4) установить флажок

«Требовать ввод имени ...», выбрать пользователя *Dispatcher*, снять флажок *«Требовать ввод имени ...»*, нажать «Применить» и в открывшемся окне указать новый пароль (который был введен ранее) для пользователя *Dispathcer*.

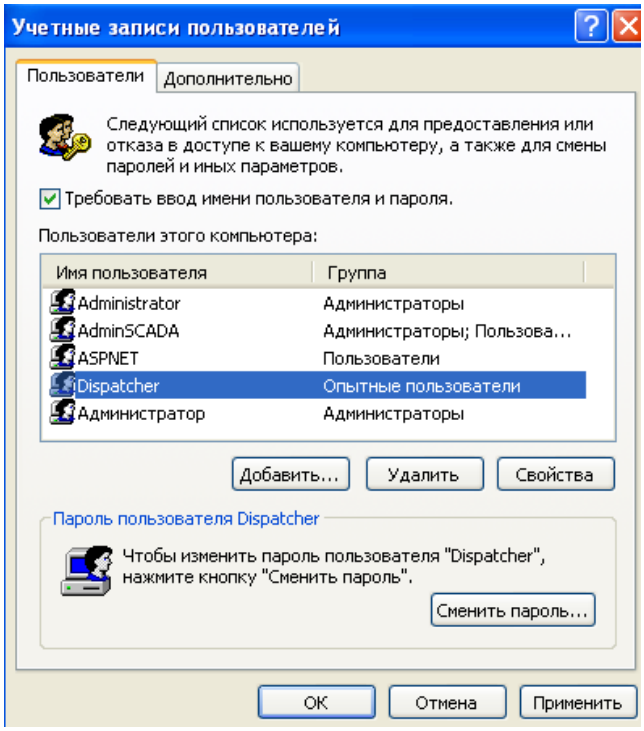

Рисунок 4 – Настройка загрузки Windows.

Внимание, если система работает в конфигурации с КИО, для упрощения настройки системы следует устанавливать одинаковые пароли для пользователей *Dispatcher*, *AdminScada* на ПК диспетчера и КИО.

2. Изменение настроек программы VNC.

Данная программа, позволяет выполнить удаленное подключение к ПК, увидеть экран ПК, и обеспечить работу с ним, так как будто вы находитесь непосредственно за компьютером. Пароль по умолчанию 0000.

2.1 Изменение пароля на доступ к программе.

Для изменения пароля, следует выбрать меню *«Пуск / Программы / RealVNC / VNC Server 4 (Service-mode) / Configure VNC Service»* в открывшемся окне, представленном на рисунке 5, выбрать вкладку *«Authentication»*, должно быть выбрано *«VNC Password ...»,* нажать *«Configure»* и ввести новый пароль.

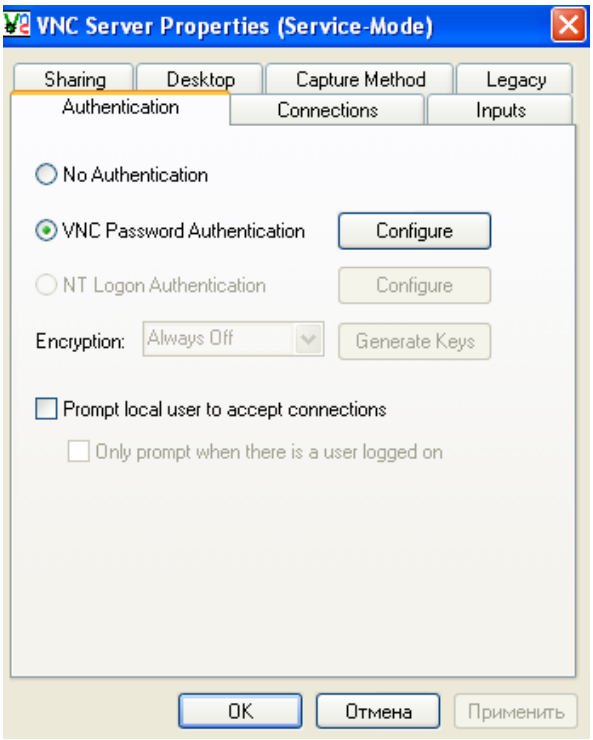

Рисунок 5 – Настройка пароля для программы VNC.

Рекомендации по выбору пароля: не менее 6 символов, чередование букв и цифр (регистр букв имеет значение, пароли «tekon» и «Tekon» - разные).

2.2 * Ограничение подключений к программе.

Программа позволяет явно указать IP-адреса компьютеров, с которых будет разрешено подключение. Доступ с других компьютеров будет блокирован, даже если известен пароль на подключение.

Данная операция значительно повышает безопасность использования программы VNC. В тоже время может ограничить вас в возможности удаленного управления ПК, если вы захотите выполнить подключение, например, с ноутбука, а не внесли его IP-адрес при настройке программы.

Для настройки ограничений следует открыть вкладку *«Connections»*, рисунок 6. По умолчанию установлен флажок *«Accept connection on Port 5900»* - принимать подключения на порт 5900, в поле *«Access Control»* «+» - принимать подключения с любых компьютеров.

Допустим необходимо сделать так, чтобы возможность подключения к данному ПК была только с удаленной машины с IP-адресом 192.168.0.54

Для этого выбираем «+» и нажимаем «*Remove*».

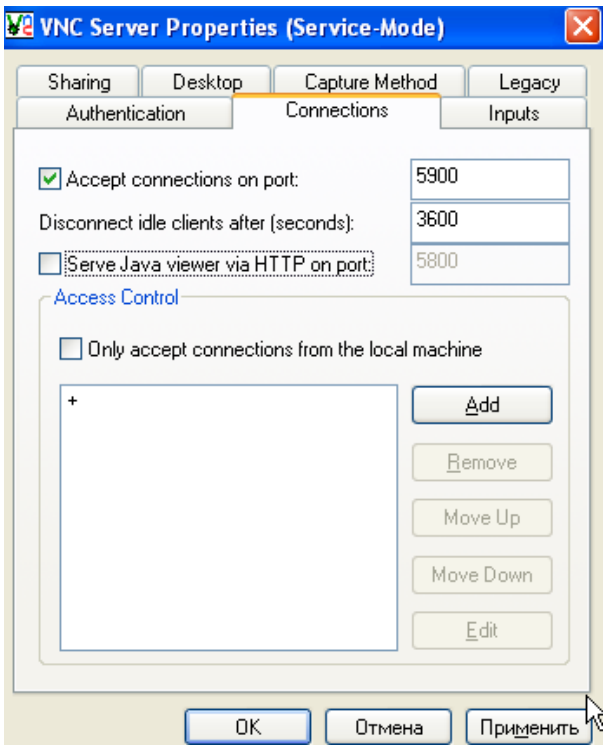

Рисунок 6 – Настройка подключений для программы VNC.

Далее нажимаем «Add». В открывшемся окне, представленном на рисунке 7, указываем *«Allow 192.168.0.54»*, нажимаем *«Ok»*.

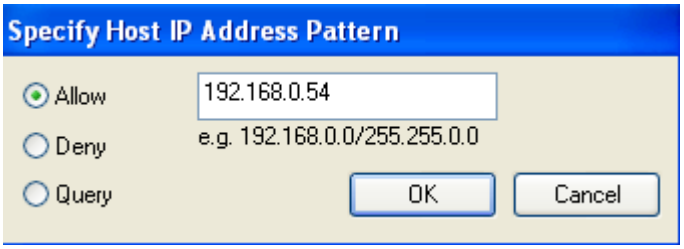

Рисунок 7 – Указание шаблона IP-адреса.

После этого в поле *«Access Control»* появится запись, как показано на рисунке 8.

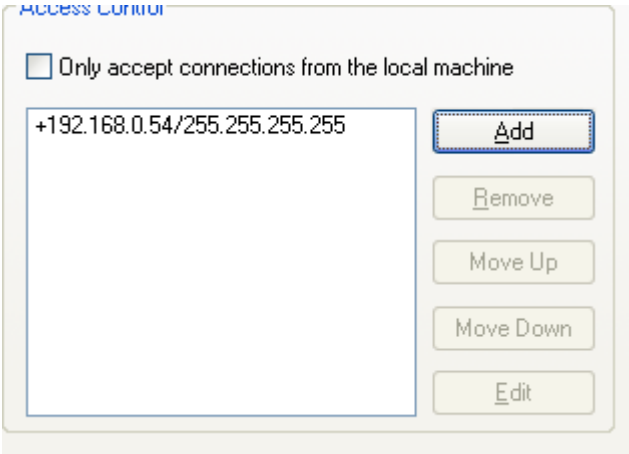

Рисунок 8 – Список разрешенных IP-адресов.

При необходимости последовательно добавляем следующие IP-адреса. Нажимаем *«Применить»*, *«Ок»*.

Более подробную информацию по настройке подключений смотри в документации на программу VNC по адресу: (*http://www.realvnc.com/products/free/4.1/winvnc.html*)

3. (*) Применение Firewall (Файрвола – межсетевого экрана).

Для предотвращения нежелательных сетевых подключений к ПК диспетчера, рекомендуется включать Firewall в настройках операционной системы, добавив исключения для программных модулей АСУД-248.

Поскольку стандартный Firewall Windows не обладает достаточной функциональностью и не всегда подходит для решения возникающих задач по обеспечению должного уровня фильтрации входящих/исходящих сетевых подключений, рекомендуется ориентироваться на сторонние программные продукты, например, *«Comodo firewall»* (настройка данного Firewall рассматривается на сайте *http://wiki.tekon.ru*)

4. (*) Применение антивирусного программного обеспечения.

Рекомендуется выполнять периодические проверки ПК диспетчера с помощью антивирусного программного обеспечения, например, «Comodo antivirus».

В случае постоянной работы антивирусного программного обеспечения следует добавить в исключение проверки папки с установленным ПО АСУД-248 («C:\1alarm», «C:\db», «C:\Program files\Tekon»).

Концентратор КУН-IP

Представляет собой устройство под управлением Unix-подобной ОС.

Настройка концентратора осуществляется по WEB-интерфейсу с помощью WEB-браузера. Для этого следует ввести IP-адрес концентратора в строке *«Адрес»* браузера, например, «*http://192.168.0.100*».

Для доступа к странице настроек по умолчанию используется логин – *«admin»*, пароль *«secret»*.

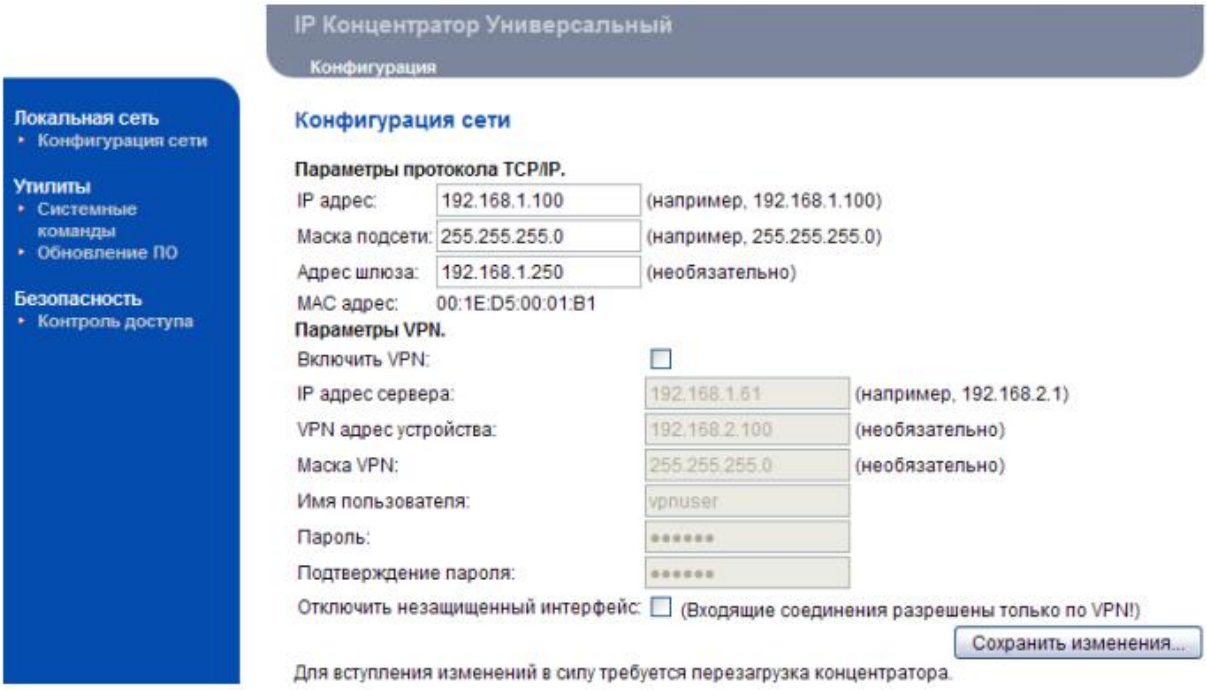

Рисунок 9 – Настройка концентратора КУН-IP.

Для изменения логина и пароля, следует войти выбрать *«Безопасность / Контроль доступа»* слева и указать новые значения логина и/или пароля.

Рекомендации по выбору пароля: не менее 6 символов, чередование букв и цифр (регистр букв имеет значение, пароли «tekon» и «Tekon» - разные).

(*) Для обеспечения безопасной работы концентратора в публичной сети следует использовать возможность концентратора выступать в качестве клиента VPN-сети (Виртуальной частной сети) и работать соответственно по защищенному VPN-соединению. Подробнее о VPN-сетях смотри соответствующую документацию.

КИО-8(4), КИО (старого типа)

Рекомендации аналогичны тем, что были рассмотрены в разделе *«ПК диспетчера»*, за исключением того, что для КИО нет необходимости авто-входа пользователя ОС после перезапуска КИО (поскольку основные программы работают как сервисы ОС).

После перезагрузки КИО должно появляться окно входа в Windows (ввод пользователя и пароля).

КИО-2М

Рекомендации аналогичны тем, что были рассмотрены в разделе *«концентратор КУН-IP»*.