Общество с ограниченной ответственностью «АСП Лабс»

Программный комплекс «Аркан»

Описание функциональных характеристик программного обеспечения

ООО «АСП Лабс»

Программный комплекс «Аркан»

Описание функциональных характеристик программного обеспечения

Тел. +7 (499) 398 00 21

http://www.asplabs.ru

Дата редакции: 15.03.2021

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	–	Автоматизированное рабочее место;
АСУ ТП	–	Автоматизированная система управления технологическим процессом;
АУД	–	Аудит безопасности;
ДМЗ	–	(Демилитаризованная зона) сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных;
ЗИС	–	Защита информационной системы и ее компонентов;
ИАФ	–	Идентификация и аутентификация субъектов доступа и объектов доступа;
ИБ	–	Информационная безопасность;
ИНЦ	–	Реагирование на компьютерные инциденты;
МЭ	–	Межсетевой экран;
ОПО	–	Управление обновлениями программного обеспечения;
ОС	–	Операционная система;
НТД	–	Нормативно-техническая документация;
ОЦЛ	–	Обеспечение целостности;
ПК	–	Программный комплекс;
ПЛК	–	Программируемый логический контроллер;
ПО	–	Программное обеспечение;
СВТ	–	Средство вычислительной техники;
СОВ	–	Система обнаружения вторжений;
СПВ	–	Средство предотвращения вторжений;
СПД	–	Система передачи данных;
УПД	–	Управление доступом субъектов доступа к объектам доступа;
УЗ	–	Устройство защиты;
ФСТЭК	–	Федеральная служба по техническому и экспертному контролю.

АННОТАЦИЯ

Настоящий документ описывает состав, основные функциональные возможности, решаемые задачи, поддерживаемые промышленные протоколы, способы развертывания и интеграции программного комплекса «Аркан» (ПК «Аркан»).

ГЛАВА 1. ВВЕДЕНИЕ

Актуальность защиты информационных процессов, протекающих в АСУ ТП, сегодня является крайней высокой проблемой, так как угрозы, исходящие от злоумышленников, постоянно усовершенствуются. Основной целью является вывести систему из строя и нанести максимально возможный ущерб (материальный, репутационный, физический и т. п.). Наиболее актуальными угрозами для АСУ ТП является сбой, отказ или нарушение режима работы; распространение вредоносного программного обеспечения.

Можно назвать основные причины, которые способствуют появлению таких угроз:

- Ошибочные действия пользователей;
- Случайный доступ посторонних лиц к системам;
- Несанкционированное подключение USB-устройств к автоматизированным рабочим местам пользователей, а также к сети Интернет.

Для минимизации угроз и обеспечении безопасности информации в целом, необходима разработка комплекса мер, с последующим внедрением. Применение систем класса СОП/СПВ для решения таких задач является одной из таких мер.

ПК «Аркан» относится к системам класса СОВ/СПВ и предназначен для использования с АСУ ТП объектов энергетики

ГЛАВА 2. ОПИСАНИЕ ПК «АРКАН»

ПК «Аркан» – программный комплекс, предназначенный для обеспечения информационной безопасности АСУ ТП. В состав ПК «Аркан» входят следующие подсистемы:

- «Аркан-М» – подсистема многофункционального межсетевого экрана (МЭ) с функцией обнаружения вторжений (далее – «Аркан-М» или устройство защиты (УЗ));
- «Аркан-К» – подсистема управления программным комплексом (далее – «Аркан-К» или сервер);
- ПО АРМ ИБ ПК «Аркан» – клиентская программа, предоставляющая интерфейс пользователю ПК «Аркан».

Архитектура ПК «Аркан» является гибко-компонуемой. В зависимости от объекта защиты, требований заказчика и др. состав и количество подсистем может отличаться.

Каждая из подсистем ПК «Аркан» представляет собой программное обеспечение, которое устанавливается на отдельную аппаратную платформу. Возможны варианты установки нескольких подсистем ПК «Аркан» на одну аппаратную платформу.

ПК «Аркан» может включать в свой состав:

- Одну подсистему «Аркан-К»;
- Одну или нескольких подсистем «Аркан-М»;
- Одну или несколько ПО АРМ ИБ ПК «Аркан».

Выявление информационных атак и инцидентов производится автоматически на основе:

- Встроенных алгоритмов;
- Базы решающих правил;
- Правил межсетевого экранирования.

Функциональные характеристики ПК «Аркан»:

- Автоматизированная инвентаризация узлов сети;
- Возможность создания и изменения правил выявления инцидентов аномалий сетевого и прикладного уровней;
- Выявление инцидентов и аномалий на прикладном уровне АСУ ТП на основе функции контроля изменения технологических параметров;

- Возможность настройки анализа промышленного трафика;
- Возможность разделения копий трафика;
- Выявление сетевых аномалий на основе правил (детектов), работающих «из коробки»;
- Контроль целостности сети (обнаружение новых устройств в сети);
- Идентификация и аутентификация пользователей;
- Возможность работы с промышленными протоколами;
- Интеграция с внешними системами класса SIEM;
- Интеграция с промышленными системами управления;
- Возможность сбора трафика без влияния на технологический сегмент, возможность работы с помощью копии трафика (SPAN/TAP);
- Динамическая визуализация сетевой топологии и сетевого взаимодействия;
- Визуализация технологического процесса в виде мнемосхемы;
- Изменение расположения элементов (динамическая, статическая привязка);
- Корреляция событий / проприетарные технологии.

2.1. ПОДСИСТЕМА АРКАН-М

Подсистема «Аркан-М» представляет собой программное обеспечение, предназначенное для решения задач межсетевого экранирования с возможностью глубокой инспекции пакетов.

Подсистема «Аркан-М» может быть настроена на работу в одном из режимов:

- Предотвращение вторжений и межсетевое экранирование (для СПВ);
- Обнаружение вторжений (для СОВ).

В случае подключения подсистемы «Аркан-М» в режиме обнаружения вторжений, коммутатор должен иметь как минимум один свободный порт для подключения, который должен быть настроен в режиме зеркалирования данных (SPAN, Port Mirroring). В данном режиме обеспечивается глубокий анализ пакетов и, в случае необходимости, отправляется уведомление оператору системы ИБ о наличии тех или иных событий или инцидентов. В данном режиме подсистема «Аркан-М» непосредственное воздействие на данные в сети не оказывает.

Преимуществом использования подсистемы «Аркан-М» в режиме предотвращения вторжений является возможность блокирования пакетов (по заданным правилам). В данном режиме подключение к сети выполняется в режиме «прозрачный мост».

Далее представлены варианты включения подсистемы «Аркан-М» при реализации СПВ и СОВ (см. Рисунок 1).

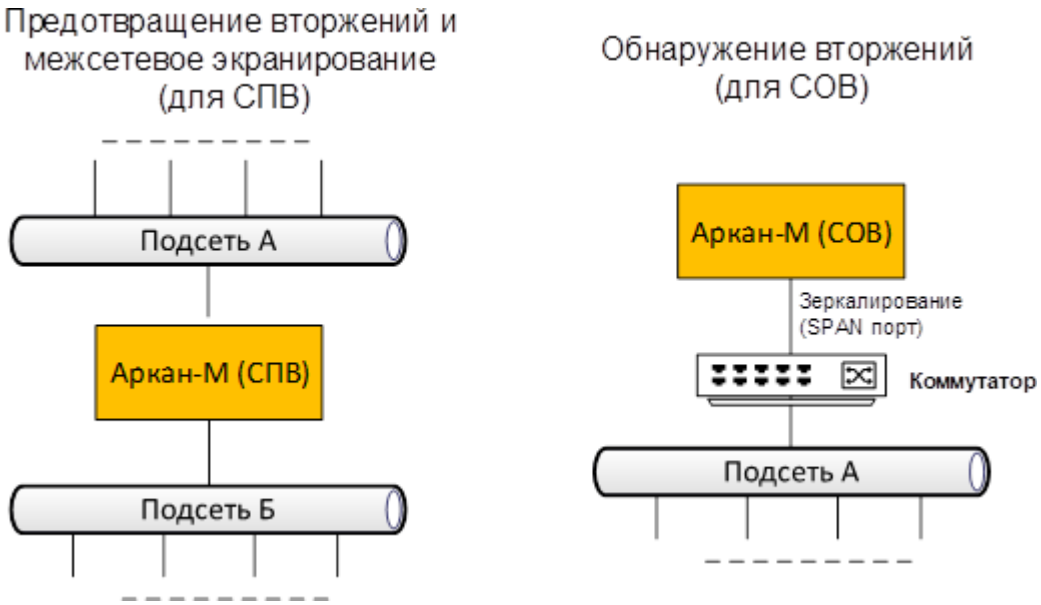

Рисунок 1. Варианты подключения подсистемы «Аркан-М»

Подсистема «Аркан-М» осуществляет анализ передаваемых в сетях пакетов данных по полям сетевого, транспортного и прикладного уровней:

- на сетевом уровне: по протоколу (например, ICMP), а также сетевым адресам;
- на транспортном уровне: на основе протоколов (UDP, TCP), а также портов источника и получателя;
- на прикладном уровне: непосредственно по полям протокола.

Поддерживаемые протоколы подсистемой «Аркан-М» для СОВ (без возможности блокирования пакетов):

- Modbus TCP;
- S7COMM;
- IEC 60870-5-104;
- OPC UA;
- OPC CLASSIC;
- IEC 61850 (MMS, GOOSE, SV);
- NTP;
- PTPv2;
- HTTP;
- FTP;
- ICMP;
- ARP;
- ряд проприетарных протоколов.

Поддерживаемые протоколы подсистемой «Аркан-М» для СПВ (с возможностью блокирования пакетов):

- Modbus TCP;
- IEC 60870-5-104;
- OPC UA;
- OPC CLASSIC;
- S7COMM.

Для протоколов доступны следующие поля для настройки:

- Название правила;

- Действие, которое необходимо произвести с пакетом данных;
- Сообщение, которое должно быть выдано при обнаружении;
- Адрес источника;
- Адрес назначения;
- Поля, зависящие от конкретного протокола.

При срабатывании установленного правила для пакета в подсистеме «Аркан-М» могут быть настроены следующие действия:

- Пропустить – прохождение пакета разрешено;
- Оповестить – информирование о срабатывании правила;
- Отклонить – блокирование и информирование о срабатывании правила;
- Удалить – блокирование пакета при срабатывании правила;

Поддерживаемые протоколы и краткие описания правил, которые могут быть применены для анализа пакетов:

- Для стандарта IEC 60870-5-104:
    1. Выбор формата пакета по типу идентификатора и команде из набора возможных для данного идентификатора: M, C, P, F;
    2. Выбор по фильтру Причины передачи;
    3. Выбор по фильтру Числового значения ASDU адреса;
    4. Выбор по фильтру Адреса объекта.
- Для стандарта IEC 61850:
    1. Выбор по фильтру PDU;
    2. Выбор по фильтру Service;
    3. Выбор по фильтру DomainID;
    4. Выбор по фильтру для ItemID.
- Для стандарта ModbusTCP:
    1. Выбор по фильтру ID устройства;
    2. Выбор по фильтру Функции;
    3. Выбор по фильтру Адреса (диапазон адресов);

4. Выбор по фильтру Доступа (чтение/запись).

- Для стандарта S7COMM:
  1. Выбор по фильтру Тип функции;
  2. Выбор по фильтру Тип сообщения.
- Для стандарта OPC UA и OPC Classic:
  1. Выбор по фильтру Тип функции;
  2. Выбор по фильтру Значение.

Подсистемой «Аркан-М» также выполняется сигнатурный анализ трафика. Для этого используются предустановленные сигнатуры (правила), позволяющие определять вредоносное воздействия. База данных сигнатур (составлена из публичных баз сигнатур) предназначена для обнаружения атак на системы общего назначения. Обновления баз данных сигнатур выполняется вручную.

При обнаружении подозрительного либо вредоносного трафика подсистема «Аркан-М» направляет информацию о нем по выделенному каналу в подсистему «Аркан-К», которая, в свою очередь перенаправляется на ПО АРМ ИБ ПК «Аркан».

В момент первого включения подсистемы «Аркан-М» необходимо задать все настройки (в том числе настройки для протоколов). Предустановленные правила по умолчанию отсутствуют.

2.2. ПОДСИСТЕМА АРКАН-К

Подсистема «Аркан-К» в части взаимодействия с подсистемой «Аркан-М» предназначена для сбора, обработки, консолидации информации и управления компонентами ПК «Аркан». Подсистема «Аркан-К» может взаимодействовать с несколькими подсистемами «Аркан-М» и ПО АРМ ИБ ПК «Аркан».

Подсистема «Аркан-К» предназначена для:

- Централизованного управления одной или несколькими подсистемами «Аркан-М»;
- Централизованного сбора и обработка информации;
- Хранения событий и инцидентов безопасности (по умолчанию глубина архива составляет 1 000 000 записей);
- Хранение конфигураций ПК «Аркан»;
- Инвентаризация информационных ресурсов (сохранение информации в БД);
- Оповещение об инцидентах в верхнеуровневые системы ИБ (SIEM).

Передача данных с ПК «Аркан» в SIEM может быть организована посредством протокола Syslog. Все события, зафиксированные системой, отправляются по протоколу Syslog в соответствии с настройками.

2.3. ПО АРМ ИБ ПК «АРКАН»

ПО АРМ ИБ ПК «Аркан» является клиентской программой, которая предназначена для предоставления графического интерфейса пользователю и управления подсистемами входящими в состав ПК «Аркан» («Аркан-М» и «Аркан-К»). При этом пользователю предоставляется унифицированный интерфейс.

ПО АРМ ИБ ПК «Аркан» предназначен для:

- Предоставления унифицированного графического интерфейса пользователю ПК «Аркан»;
- Настройка и управление «Аркан-К» и «Аркан-М» (возможность управления несколькими «Аркан-М»);
- Оповещение об инцидентах ИБ;
- Отображение системных событий ПК «Аркан» и событий наблюдаемой сети;
- Управление инцидентами.

ПО АРМ ИБ ПК «Аркан» может быть установлена как на отдельную аппаратную платформу, так и совместно с подсистемой «Аркан-К».

Интерфейс ПО АРМ ИБ ПК «Аркан» (см. Рисунок 2) состоит из главного экрана, предназначенного для быстрого доступа к необходимой информации, который включает в себя:

- Панель навигации (справа),
- Индикаторы состояния системы (верхняя часть),
- Индикаторы уведомлений (справа сверху),
- Информационную строку (снизу)
- Рабочую область.

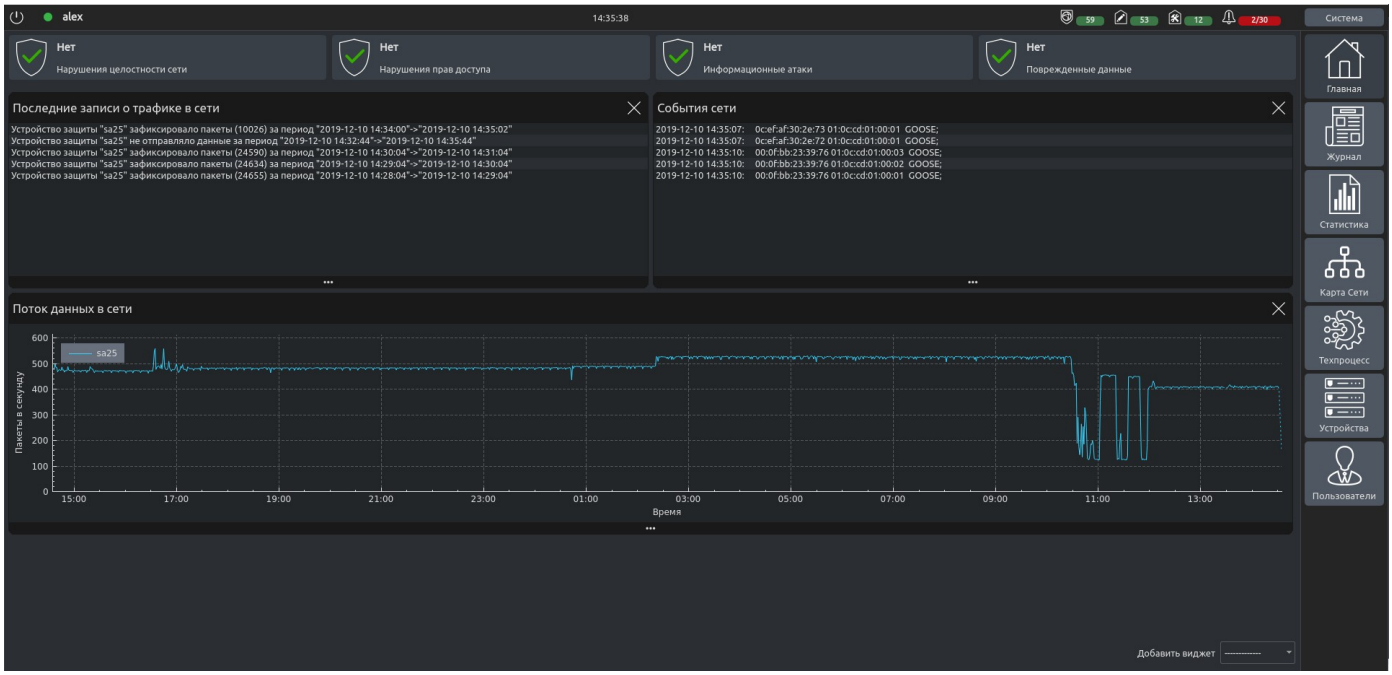

Рисунок 2. Вид главного экрана ПО АРМ ИБ ПК «Аркан»

Вариант окна «Карта сети» представлен на рисунке (Рисунок 3).

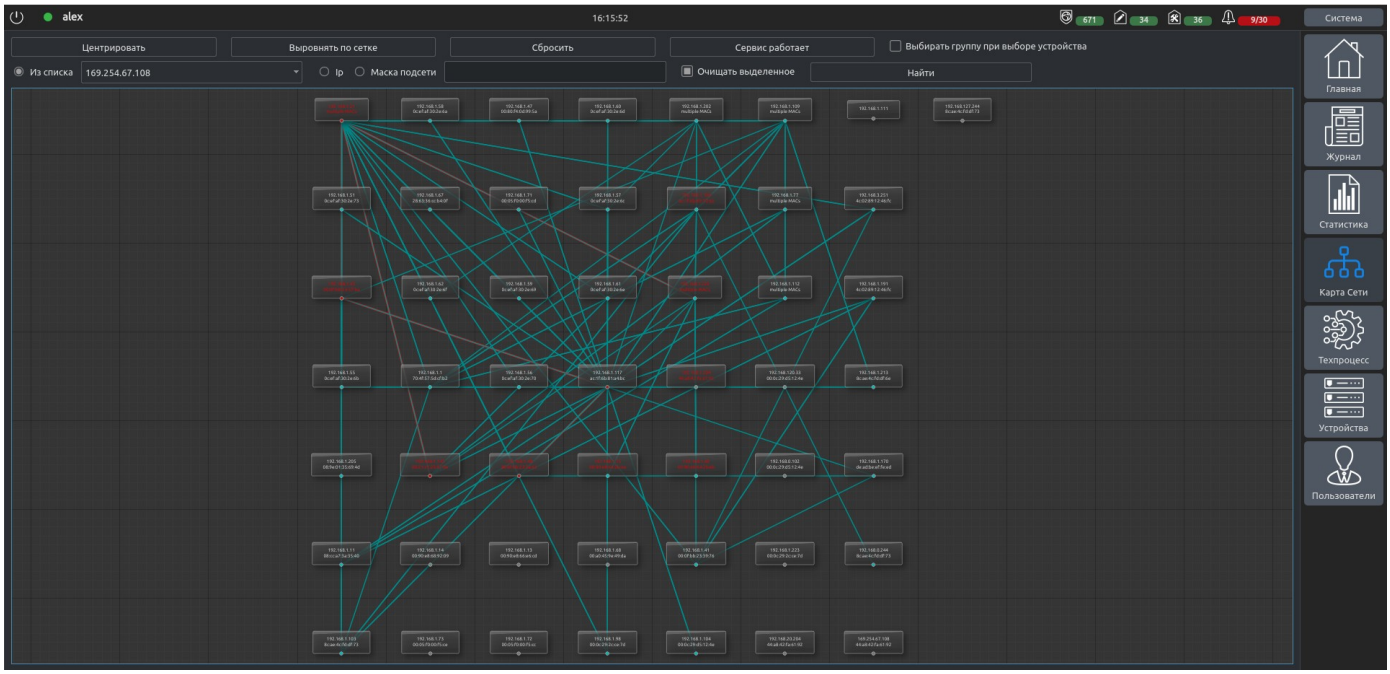

Рисунок 3. Вид окна «Карта сети»

В ПО АРМ ИБ ПК «Аркан» предусмотрена возможность отображения мнемосхемы технологического процесса контролируемого объекта.

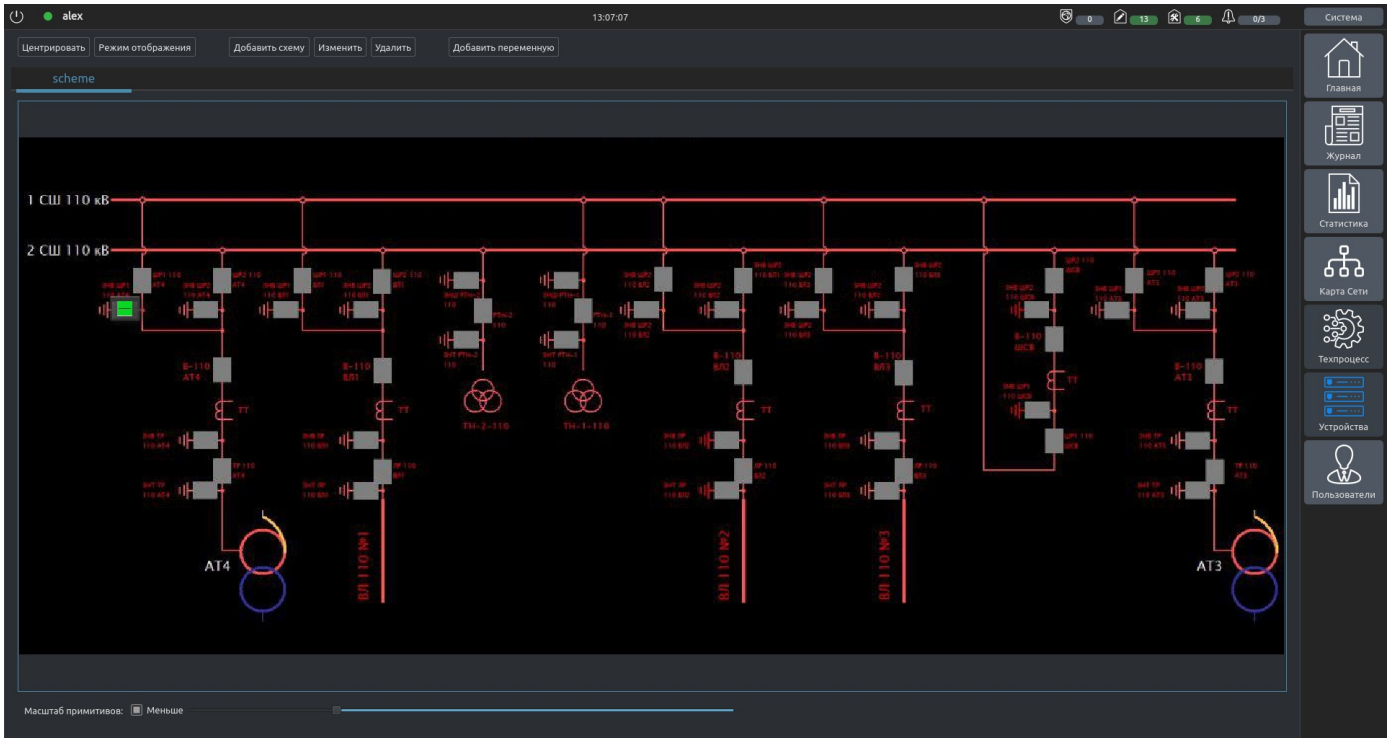

Рисунок 4. Вид окна «Техпроцесс»

ГЛАВА 3. ВАРИАНТЫ ПРИМЕНЕНИЯ ПК «АРКАН»

В зависимости от различных факторов, таких как: особенности технологического процесса, требований НТД или заказчика, бюджета проекта и т.д. – могут применяться различные варианты развертывания подсистем ПК «Аркан».

Развертывание ПК «Аркан» для реализации СОВ

Подсистема «Аркан-М» подключается к контролируемому сегменту сети через SPAN порт коммутатора. Сетевые интерфейсы в подсистеме «Аркан-М» настроены в режим обнаружения вторжений, тем самым реализуется СОВ. При обнаружении подозрительного либо вредоносного трафика подсистема «Аркан-М» отправляет информацию о нем по шине ДМЗ на сервер ПК «Аркан» (в подсистему «Аркан-К»). После чего данная информация доступна для отображения в клиентской программе ПО АРМ ИБ ПК «Аркан». Подсистема «Аркан-М» функционирует в пассивном режиме и не воздействует на трафик внутри контролируемого сегмента сети (см. Рисунок 5).

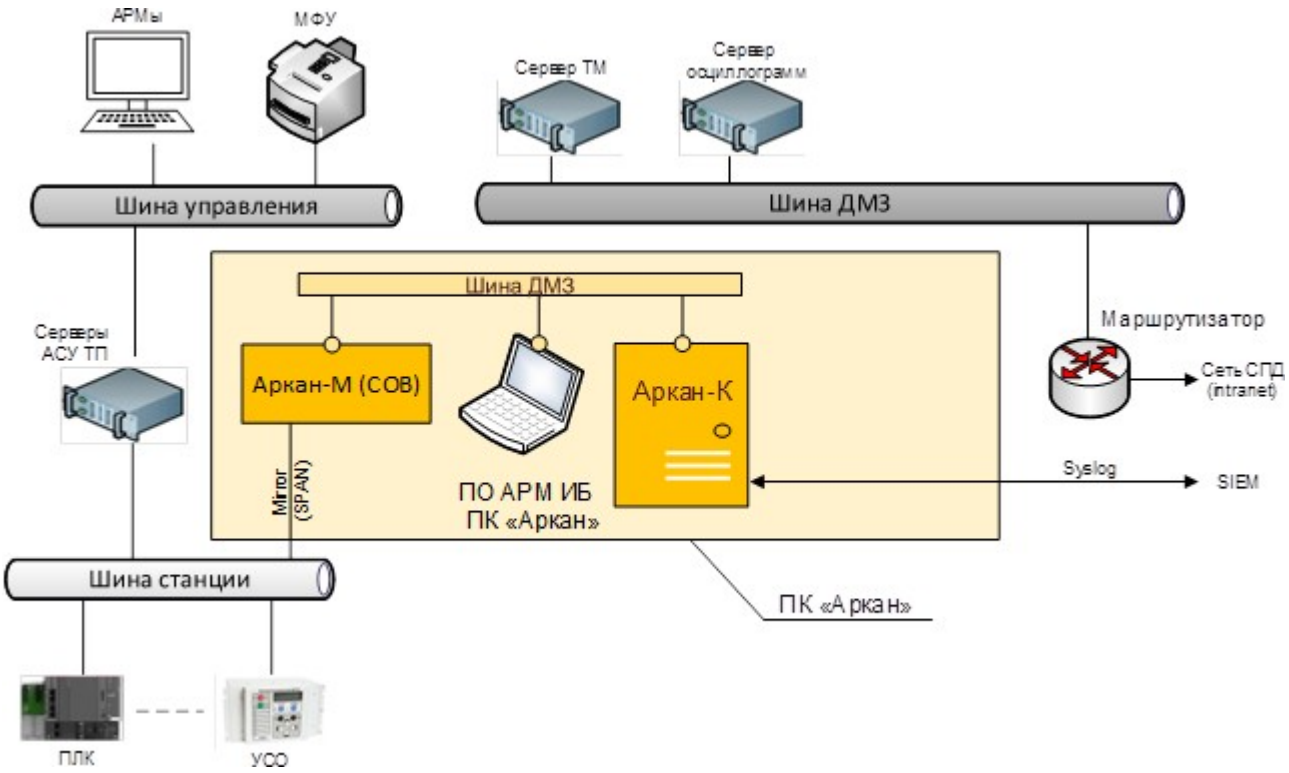

Рисунок 5. Развертывание ПК «Аркан» для реализации СОВ

Развертывание ПК «Аркан» для реализации СПВ

Подсистема «Аркан-М» устанавливается в разрез между маршрутизатором и остальными устройствами выбранного сегмента сети. Сетевые интерфейсы в подсистеме «Аркан-М» настроены в режим предотвращения вторжений и межсетевого экранирования, тем самым реализуется СПВ. При обнаружении подозрительного либо вредоносного трафика подсистема «Аркан-М» отправляет информацию о нем по шине ДМЗ на сервер ПК «Аркан» (в подсистему «Аркан-К»), а также может заблокировать передачу пакетов (при необходимости). После попадания в подсистему «Аркан-К» информация доступна для отображения в клиентской программе ПО АРМ ИБ ПК «Аркан» (см. Рисунок 6).

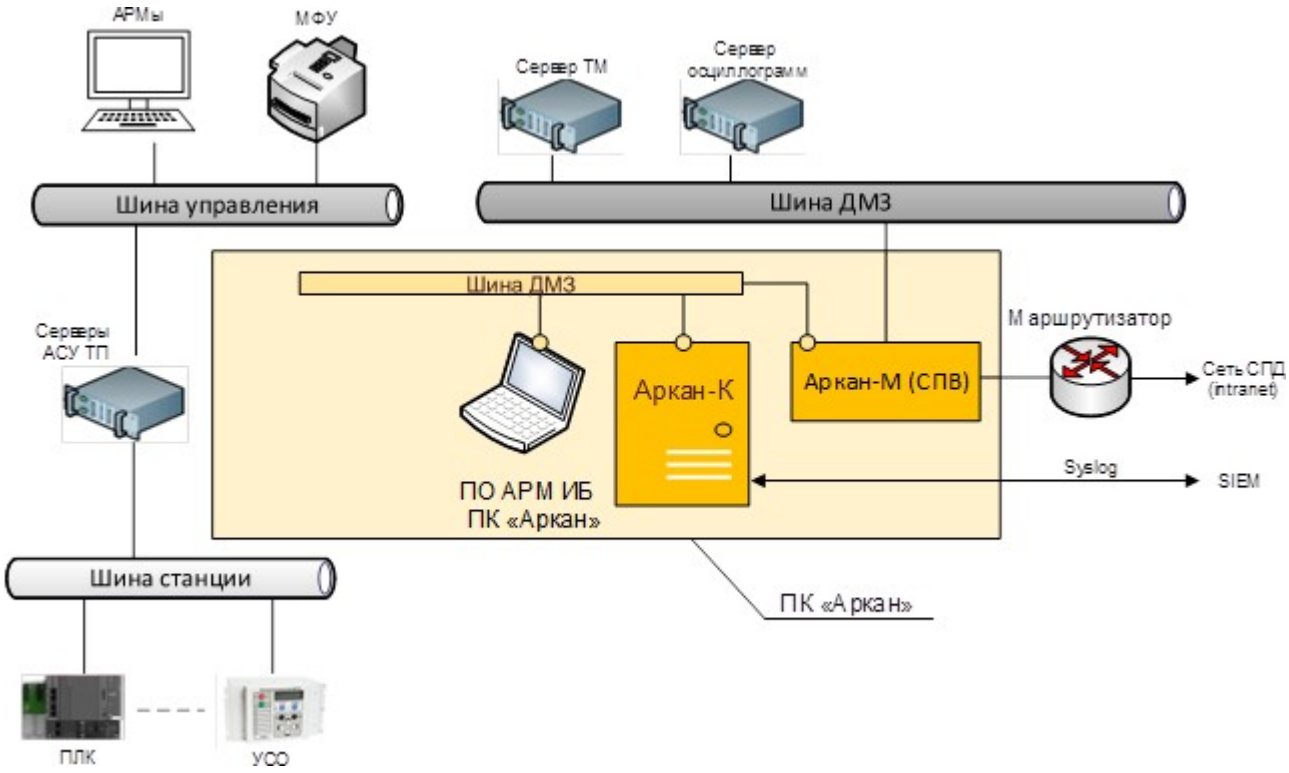

Рисунок 6. Развертывание ПК «Аркан» для реализации СПВ

Развертывание ПК «Аркан» для реализации СОВ и СПВ

В данном варианте одна из подсистем «Аркан-М» устанавливается в разрез между маршрутизатором и остальными устройствами выбранного сегмента сети (СПВ), другая подключается к контролируемому сегменту сети через SPAN порт коммутатора. Каждая подсистема настраивается на свой режим работы. При обнаружении подозрительного либо вредоносного трафика подсистема «Аркан-М» отправляет информацию о нем по шине ДМЗ на сервер ПК «Аркан» (в подсистему «Аркан-К»), а также может заблокировать передачу пакетов (для СПВ). После попадания в подсистему «Аркан-К» информация доступна для отображения в клиентской программе ПО АРМ ИБ ПК «Аркан» (см. Рисунок 7).

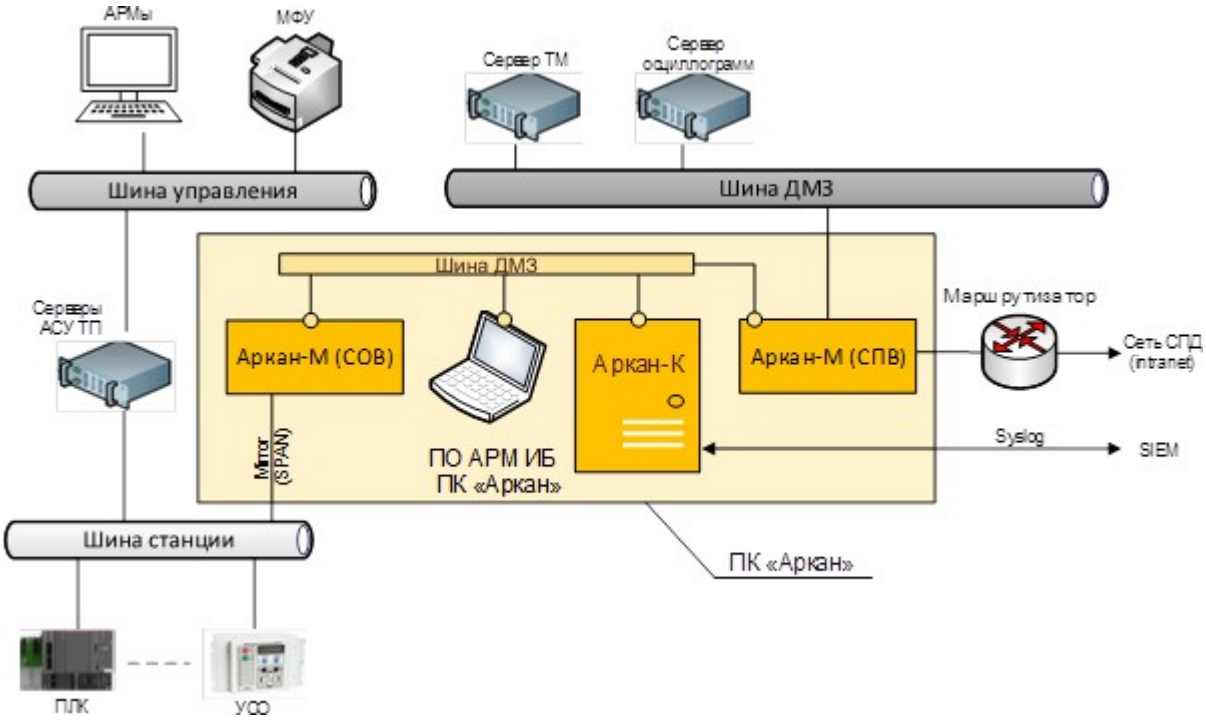

Рисунок 7. Развертывание ПК «Аркан» для реализации СОВ и СПВ

Вариант развертывания ПК «Аркан» для АСУ ТП электрической подстанции. На рисунке ниже (см. Рисунок 8) представлен вариант развертывания ПК «Аркан» для применения в АСУ ТП электрической подстанции.

В данном варианте структуры ПК «Аркан» состоит из следующего набора подсистем:

- Подсистема «Аркан-К» - 1 комплект;
- Подсистема «Аркан-М» (режим работы СПВ) - 2 комплекта;
- Подсистема «Аркан-М» (режим работы СОВ) - 2 комплекта;
- ПО АРМ ИБ ПК «Аркан» - 1 комплект.

Подсистемы «Аркан-М» (СОВ-1 и СОВ-2) работают с копией трафика наблюдаемой сети (полученным с интерфейсов зеркалирования коммутаторов уровня доступа хостов АСУ ТП). Подсистемы «Аркан-М» (СПВ-1 и СПВ-2) работают в режиме «прозрачный мост». Данное подключение обеспечивает сегментирования ЛВС АСУ ТП и системы передачи технологической информации (СПД), глубокой инспекции пакетов промышленных протоколов и фильтрацию трафика.

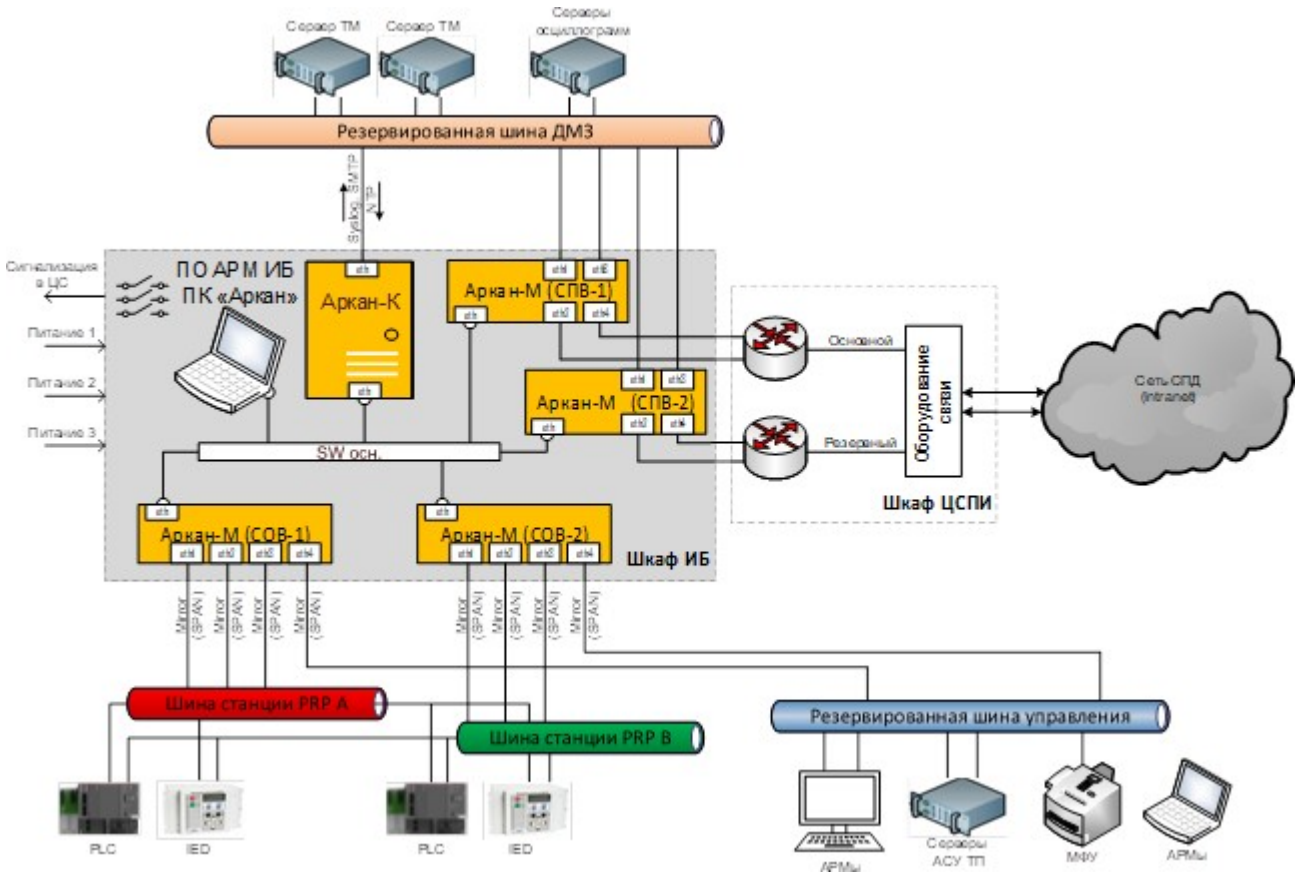

Рисунок 8. Вариант развертывания ПК «Аркан» для АСУ ТП подстанции

ГЛАВА 4. ТРЕБОВАНИЯ К АППАРАТНЫМ СРЕДСТВАМ ПК «АРКАН»

Минимальные параметры СВТ для установки подсистем ПК «Аркан» представлены в таблице ниже (см. Таблица 1)

Таблица 1. Минимальные параметры аппаратных (технических) средств для установки подсистем ПК «Аркан»

Наименование подсистемы ПК «Аркан»	Технические характеристики
ПО АРМ ИБ ПК «Аркан»	- Процессор - Intel Core i3 2400 МГц и выше; - Оперативной памяти - 1 Гб или больше; - Жесткий диск - 60 Гб или больше, SATA/SCSI; - Сетевое оборудование – наличие не менее одного сетевого интерфейса 100/1000 Base-T; - ОС Debian 9 (и выше) или Windows 10.
«Аркан-К»	- Процессор - Intel Core i5 2400 МГц и выше; - Оперативной памяти - 8 Гб или больше; - Жесткий диск - 60 Гб или больше, SATA/SCSI; - Сетевое оборудование – наличие не менее одного сетевого интерфейса 100/1000 Base-T; - ОС Debian 9 (и выше).
«Аркан-М»	- Процессор - Intel Core i5 2400 МГц и выше; - Оперативной памяти - 8 Гб или больше; - Жесткий диск - 60 Гб или больше, SATA/SCSI; - Сетевое оборудование – наличие не менее 3-х сетевых интерфейсов 100/1000 Base-T; - ОС Debian 9 (и выше);

ГЛАВА 5. СООТВЕТСТВИЕ НТД

ПК «Аркан» соответствует требованиям ФСТЭК России, которые представлены в документах:

- «ИТ.СОВ.У4.ПЗ Методический документ. Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты»
- «ИТ.МЭ.Д4.ПЗ. Методический документ. Профиль защиты межсетевых экранов типа "Д" четвертого класса защиты»

Меры обеспечения ИБ реализованные в ПК «Аркан» в соответствии с:

- Приказом Федеральной службы по техническому и экспортному контролю 239 от 25 декабря 2017 года «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (см. Таблица 2);
- Приказом 31 от 14 марта 2014 года «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Таблица 2. Функционал ПО

Обозначение и номер меры	Функционал
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов.
ИАФ.3	Управление идентификаторами.
ИАФ.7	Защита аутентификационной информации при передаче. При любой аутентификации используются сертификаты.
Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление учетными записями пользователей. Создание, удаление и изменение учётных записей пользователей.
УПД.2	Реализация политик управления доступа. Возможно задание уровня доступа пользователя.
УПД.4	Разделение полномочий (ролей) пользователей. Операции, проводимые пользователем, разделены по уровням доступа.

Обозначение и номер меры	Функционал
УПД.5	Назначение минимально необходимых прав и привилегий. При создании пользователя, наделяется минимальными правами доступа.
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему.
УПД.9	Ограничение числа параллельных сеансов доступа.
Аудит безопасности (АУД)	
АУД.1	Инвентаризация информационных ресурсов. Проводится построение карты сети в пассивном режиме и опрос устройств по SNMP. Определяется и отображается: - Информация об устройствах (IP-адрес, MAC-адрес, производитель сетевого оборудования, операционная система, время первой и последней активности) - Информация о связях между устройствами (протоколы, трафик, время первой и последней активности) - Информация текущих сетевых соединениях
АУД.2	Анализ уязвимостей и их устранение. Обнаруживаются и предотвращаются атаки на известные уязвимости.
АУД.3	Генерирование временных меток и (или) синхронизация системного времени. Задание времени, синхронизация времени по протоколу NTP.
АУД.4	Регистрация событий безопасности. События безопасности заносятся в соответствующий журнал.

Обозначение и номер меры	Функционал
АУД.5	Контроль и анализ сетевого трафика. Протоколы, для которых возможно оповещение об атаках (СОВ): - Modbus TCP; - S7COMM; - IEC 60870-5-104; - OPC UA; - OPC CLASSIC; - IEC 61850 (MMS, GOOSE, SV); - NTP; - PTPv2; - HTTP; - FTP; - ICMP; - ARP; - ряд проприетарных протоколов. Протоколы, для которых возможно предотвращение атак (СПВ): - Modbus TCP; - IEC 60870-5-104; - OPC UA; - OPC CLASSIC; - S7COMM.
АУД.6	Защита информации о событиях безопасности. Информация о событиях безопасности доступна авторизованным пользователям.
АУД.9	Анализ действий отдельных пользователей. Все действия пользователей сохраняются в системный журнал.
Предотвращение вторжений (компьютерных атак) (СОВ)	
СОВ.1	Обнаружение и предотвращение компьютерных атак. Обнаруживаются следующие виды атак: - Обнаружение незарегистрированных сетевых устройств; - Обнаружение факта «Сканирование сети»; - Обнаружение атаки ARP-Spoofing; - Обнаружение атаки «Flooding»; - Обнаружение атаки «Эксплуатация известных уязвимостей»; - Обнаружение использования запрещенных политикой функций промышленных протоколов; - Обнаружение изменения программы управления ПЛК, атак на изменение параметров ПЛК в том числе по промышленным протоколам; - Обнаружение запрещенного политикой информационного потока (на основании протокола, адресов источника и назначения).

Обозначение и номер меры	Функционал
СОВ.2	Обновление базы решающих правил.
Обеспечение целостности (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения. Контроль целостности файлов ПК осуществляется периодически.
ОЦЛ.2	Контроль целостности информации. выполняется для ряда промышленных протоколов (MMS, GOOSE,SV).
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях. Восстановление базы данных из резервной копии проводится по запросу пользователя.
ОЦЛ.6	Обезличивание и (или) деидентификация информации. Как ПК в целом, таки и отдельные его сервисы, перезапускаются после сбоя без вмешательства оператора.
Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	
ЗИС.19	Защита информации при ее передаче по каналам связи. Вся информация между подсистемами ПК передаётся с использованием шифрования.
Реагирование на компьютерные инциденты (ИНЦ)	
ИНЦ.1	Выявление компьютерных инцидентов. Инциденты выявляются на основании функционирования ряда служб (межсетевой экран, СОВ, модуль контроля целостности и другие).
ИНЦ.2	Информация о компьютерных инцидентах. Инцидент помещается в соответствующую группу, которая впоследствии может быть помечена как подлежащая игнорированию или решённая, возможна передача инцидентов на email по протоколу SMTP.
ИНЦ.3	Анализ компьютерных инцидентов. При отображении инцидента выводится технический комментарий, содержащий детали инцидента.
Управление обновлениями программного обеспечения (ОПО)	
ОПО.4	Обновление осуществляется удалённо, с использованием компьютера-установщика.