УТВЕРЖДЕН
11443195.4012-053 ИЗ 2012 ЛУ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

«АККОРД-РАУ»

Руководство Оператора

Листов 14

Москва

2020

АННОТАЦИЯ

Специальное программное обеспечение (СПО) средств защиты информации от несанкционированного доступа «Аккорд-РАУ» (далее – «Аккорд-РАУ», РАУ) предназначено для централизованного мониторинга событий ИБ и управления средствами защиты информации от несанкционированного доступа (СЗИ НСД) «Аккорд».

Данный документ описывает действия Оператора, связанные с непосредственной эксплуатацией системы информационной безопасности (далее – система) в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение

1.1 Область применения

Деятельность Оператора РАУ.

1.2 Функции Оператора РАУ

Оператор РАУ выполняет следующие функции:

- обеспечивает мониторинг взаимодействия и функционирования технических и программных средств РАУ;
- регистрирует нештатные ситуации на КТС РАУ, КТС смежных подсистем, на которых размещены компоненты РАУ, или каналах их взаимодействия и уведомляет о них Администратора РАУ.

1.3 Комплект поставки

В комплект поставки РАУ входят следующие компоненты:

– сервер централизованного управления (СЦУ) с предустановленными СЗИ от НСД и ПО сервера централизованного управления;

– клиентские компоненты (сетевые агенты), устанавливаемые на подконтрольных объектах (ПКО);

– лицензии на подключение подконтрольных объектов к РАУ на touch memory (далее – TM) типа DS 1996;

- комплект рабочей документации на компакт диске (далее – CD).

2 Назначение и условия применения

2.1 Назначение

РАУ обеспечивает:

- централизованный сбор и хранение информации о зарегистрированных событиях доступа к подконтрольным объектам;
- возможность централизованного управления СЗИ от НСД «Аккорд» на подконтрольных объектах;
- единую точку контроля доступа к периферийным устройствам и контроля использования отчуждаемых машинных носителей.

2.2 Условия применения

Условия применения компонентов РАУ приведены в документе «11443195.4012-053 90. СПО СЗИ НСД «Аккорд-РАУ». Руководство Администратора».

3 Порядок работы

Оператор РАУ обеспечивает мониторинг взаимодействия и функционирования технических и программных средств системы.

Оператор регистрирует нештатные ситуации на комплексе технических средств (КТС) системы, КТС смежных подсистем, на которых размещены компоненты РАУ, или каналах их взаимодействия и уведомляет о них администратора РАУ.

Для проверки работоспособности ПАК СЗИ от НСД «Аккорд» на ПКО, а также для обеспечения синхронизации баз СЗИ от НСД «Аккорд» и обновления агентов РАУ на ПКО Оператор РАУ обеспечивает загрузку ПКО до этапа входа в ОС Windows. Для этого на ПКО создается групповая учетная запись Оператора РАУ с правами пользователя в «Аккорд-АМДЗ» и не имеющая прав на вход в ОС Windows. ТМ-идентификатор данной учетной записи должен храниться в сейфе подразделения, сотрудники которого назначены на роль Оператора РАУ, и передаваться по журналу.

4 Перечень оповещающих сообщений

Оповещающие сообщения выводятся только на экран и не фиксируются ни в каких журналах. Перечень оповещающих сообщений, действия, при которых генерируются данные сообщения, а также действия, которые необходимо предпринять при появлении данных сообщений, приведены в таблице 1.

Таблица 1 - Перечень оповещающих сообщений

Сообщение	**Действия, при которых генерируется сообщение**	**Действия, которые необходимо предпринять при появлении сообщения**
«Ошибка чтения ТМ…» (на красном фоне)	В ответ на запрос ТМ-идентификатор был неправильно прислонен к съемнику информации	Снова приложите ТМ-идентификатор к съемнику информации после появления нового запроса
«Это не сетевой ТМ»	В ответ на запрос был прислонен ТМ-идентификатор, не содержащий необходимой информации	Прислонить сетевой ТМ-идентификатор
«В данное время вход в систему запрещен»	Попытка войти в систему в то время, когда работа запрещена настройкой временных ограничений	Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка) и уточнить разрешенное время работы и в случае возможности и необходимости скорректировать временные ограничения. Процедура установки временных ограничений описана в документации ПАК СЗИ от НСД «Аккорд»
«Ваш пароль просрочен. Обратитесь к администратору для смены» (на красном фоне)	Попытка войти в систему, используя просроченный пароль или закончились все попытки смены пароля	Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка) для смены пароля

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
«Доступ не разрешен!» (на красном фоне)	Использован недопустимый идентификатор пользователя или введен неправильный пароль при попытке входа в систему	Повторить попытку процедуры идентификации / аутентификации, если не поможет обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
«Требуется Администратор» (на красном фоне) «Разберитесь с ошибками» (на оранжевом фоне)	Попытка пользователя войти в систему	Несовпадение контрольных и текущих параметров аппаратной и программной частей системы. Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка) для выявления и устранения причины изменения параметров
«Такую комбинацию символов недопустимо использовать в качестве пароля»	Попытка пользователя сменить пароль	Пользователь пытается задать в качестве нового пароля комбинацию символов, которую легко подобрать, например, qwerty. Необходимо ввести более сложную комбинацию символов. Желательно, чтобы пароль содержал цифры, буквы верхнего и нижнего регистра, а его длинна была не менее восьми символов
«Отсутствует разрешение на смену пароля»	Попытка пользователя сменить пароль	У пользователя нет прав на смену пароля. Необходимо обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
В идентификаторе нет свободных страниц для записи»	Попытка регистрации 32-ой рабочей станции без сохранения списка на сервере централизованного управления и очистки памяти ТМ	Объем идентификатора DS1996 позволяет хранить данные о 31 рабочей станции и их открытые ключи. Если в сети остались незарегистрированные станции, то следует добавить список на сервере централизованного управления и после очистки памяти ТМ провести регистрацию остальных рабочих станций
«ВНИМАНИЕ! Станция имеет адрес 127.0.0.1. Скорее всего она не подключена к сети. Вы желаете продолжить регистрацию станции?»	Попытка регистрации рабочей станции с IP-адресом 127.0.0.1	Необходимо нажать кнопку <Нет> в появившемся сообщении. Выполнить процедуру регистрации, убедившись, что между ПКО и ASM существует сетевое соединение
Доступ запрещен	Попытка исполнения функции без соответствующих прав при работе по централизованной схеме	Если нет необходимости в доступе к данному ресурсу, и попытка доступа была предпринята по ошибке, то никаких действий предпринимать не нужно. Если же необходим доступ к данному ресурсу, то следует обратиться к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
Заполните все необходимые поля	Не заполнен пароль при попытке авторизации в автономном режиме	Введите пароль

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
Ошибка получения XID	При попытке авторизации не были получены XID – данные учетной записи ASM, необходимые для записи базы в плату на ПКО. Причинами данной ошибки могут являться проблемы со связью (сетью) на момент запроса XID или отсутствие на сервере централизованного управления учётной записи ASM	1 Проверьте наличие связи межу сервером централизованного управления и ПКО. При отсутствии связи, восстановите ее. 2 Обратитесь к Администратору ИБ для проверки существования на сервере централизованного управления учётной записи ASM, под которой произошла данная ошибка
Ошибка чтения ТМ-идентификатора	При работе в автономном режиме в ответ на запрос ТМ-идентификатор был неправильно прислонен к съемнику информации	Снова приложите ТМ-идентификатор к съемнику информации после появления нового запроса
Отправлена база пользователей	При работе в автономном режиме отправлена база пользователей	Данное сообщение информирует об успешной отправке базы пользователей в автономном режиме. Никаких действий при его появлении выполнять не нужно
Файлы баз были экспортированы	При работе в автономном режиме выполнен экспорт файлов	Данное сообщение информирует об успешном экспортировании файлов баз в автономном режиме. Никаких действий при его появлении выполнять не нужно
Файлы баз были импортированы	При работе в автономном режиме выполнен импорт файлов	Данное сообщение информирует об успешном импортировании файлов баз в автономном режиме. Никаких действий при его появлении выполнять не нужно

Сообщение	Действия, при которых генерируется сообщение	Действия, которые необходимо предпринять при появлении сообщения
База пользователей не применена, откат к предыдущей версии	Попытка обновления базы пользователей	Повторите попытку обновления базы пользователей, если и повторная попытка окажется неудачной, получите новую базу пользователей и повторите попытку обновления, если и это не поможет, обратитесь к Администратору ИБ средств защиты информации от НСД (АИБ технологического участка)
Файлы журналов были экспортированы	При работе в автономном режиме выполнен экспорт файлов журналов	Данное сообщение информирует об успешном экспортировании файлов журналов в автономном режиме. Никаких действий при его появлении выполнять не нужно
Отсутствует файл учетной записи ASM. Выполните настройку и запустите службу AcConNet!	После установки сервера централизованного управления при первом его запуске не была сразу же выполнена предварительная настройка сетевого идентификатора	Выполнить предварительную настройку сетевого идентификатора и запустить службу AcConNet

5 Перечень принятых сокращений

АИБ	Администратор информационной безопасности
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
КТС	Комплекс технических средств
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
НШР	Нештатный режим
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
РАУ	Распределенный Аудит и Управление
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СУ	Система управления

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	замененных	новых	аннулированных					

СОГЛАСОВАНО

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата