INTEGRITY SCADA
ПЕРВОЕ РЕШЕНИЕ В ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ СЕРТИФИЦИРОВАННОЕ ФСТЭК

ЭЛЕСИ 35

ПРОГРАММНО ИНСТРУМЕНТАЛЬНЫЙ КОМПЛЕКС ДЛЯ СОЗДАНИЯ СИСТЕМ УПРАВЛЕНИЯ И АВТОМАТИЗАЦИИ НА БАЗЕ СВОБОДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

РЕЕСТР РОССИЙСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ГОСУДАРСТВЕННЫЙ РЕЕСТР СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Реестровая запись №5671 согласно базы данных ФСТЭК России уязвимости в программном комплексе отсутствуют

Программный комплекс разработан в соответствии с требованиями безопасной разработки программного обеспечения: лицензия на деятельность по технической защите конфиденциальной информации ФСТЭК России №Л024-00107-00/00583124, лицензия на деятельность по разработке и производству средств защиты конфиденциальной информации ФСТЭК России №Л050-00107-00/00584020

Уровень информационной безопасности компонент программного комплекса соответствует требованиям по обеспечению безопасности применяемых на объектах критической информационной инфраструктуры (КИИ) 1, 2, 3 категории значимости

Уровень информационной безопасности Integrity SCADA соответствует требованиям по обеспечению безопасности значимых объектов КИИ Российской Федерации (Приказ № 239 ФСТЭК России от 25.12.2017), в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Сертификат соответствия № 4935 по безопасности информационных технологий по 4 уровню доверия


ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ


ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО РАЗРАБОТКЕ И ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ИСПОЛНЕНИЕ ТРЕБОВАНИЙ ПОСТАНОВЛЕНИЯ ПРАВИТЕЛЬСТВА РФ № 1912 от 14.11.2023 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации»

Минцифры России

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

scadaint.ru

634000, Россия, Томск,
ул. Алтайская, 161А
тел.: +7 (3822) 601-000, 499-200
e-mail: int@scadaint.ru
elesy@elesy.ru

ВСТРОЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В INTEGRITY SCADA

IntegrityClientSecurity – обеспечение функции клиентской безопасности

Назначение:
Управление правами доступа пользователей к функциям клиентских приложений SCADA-системы

Основные функции

- администрирование прав доступа;
- ограничение прав пользователей на использование клиентских приложений программного комплекса;
- ограничение периода работы пользователей по времени;
- предоставление пользователям и группам пользователей разрешений на использование отдельных предварительно заданных функций клиентских приложений;
- автоматическая авторизация пользователя одновременно в нескольких клиентских приложениях в рамках одного или нескольких компьютеров.

Особенности

- использование кроссплатформенных служб организации учетных записей пользователей;
- распределенная система резервирования;
- возможность объединения нескольких компьютеров в кластер и последующая совместная работа со всеми компьютерами кластера;
- обеспечение методов аутентификации пользователей как в рамках рабочих групп, так и в рамках доменной сети предприятия.

Удобство настройки

- настройка прав пользователей для работы с клиентскими приложениями Integrity SCADA возможна по перечню приложений, функциям приложений и временным интервалам;
- визуальные средства администрирования и управления правами доступа пользователей позволяют легко настраивать права доступа и временные интервалы как для каждого пользователя, так и для групп;
- осуществление контроля прав и аудита доступа к различным защищаемым ресурсам системы управления технологическими процессами, таким как экраны, слои, данные и пр.;
- добавление пользовательских функций.

IntegrityEnvironmentControl – контроль целостности файлов проекта и системы

Назначение:
Организация сбора диагностической информации по контролю целостности программной среды, событиям, файлам, папкам, службам и процессам, с дальнейшим предоставлением данных по OPC UA

Основные функции

- контроль целостности файлов по контрольной сумме, времени изменения, размеру, атрибутам;
- контроль изменения содержимого папки;
- расчет контрольной суммы файла с использованием алгоритмов ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 (с длиной хэш-кода 256/512);
- формирование диагностики ПК: память, диск, сеть, загрузка ЦПУ, температурные датчики;
- слежение за процессами (количество экземпляров и загрузка ЦПУ);
- предоставление данных и управление контролем по протоколу OPC UA;
- формирование отчета с указанием контрольных сумм;
- журналирование всех действий пользователя при работе с компонентой;
- конфигурация компоненты зашифрована; удобное конфигурирование в графическом приложении.

Особенности

- использование кроссплатформенных служб организации учетных записей пользователей;
- распределенная система резервирования;
- возможность объединения нескольких компьютеров в кластер и последующая совместная работа со всеми компьютерами кластера;
- обеспечение методов аутентификации пользователей как в рамках рабочих групп, так и в рамках доменной сети предприятия.

Нативный кроссплатформенный код на C++
Собственная реализация межпроцессного взаимодействия
Собственная NoSQL СУБД хранения временных рядов и таблиц
Единая шина данных на основе открытого стандарта OPC UA
Собственный framework

Полностью управляемый исходный код
Интегрированная киберзащита АСУ ТП
Безопасность встроена, а не добавлена
Исполнение функции ИБ для среднего и верхнего уровня АСУ ТП
Сертифицированные встроенные СЗИ

Безопасность передаваемых данных

- Использование безопасного протокола передачи данных во всех компонентах комплекса;
- Поддержка всех актуальных политик безопасности в соответствии со спецификацией OPC UA;
- Интеграция и передача данных в сторонние SIEM;
- Ограничение подключения;
- Подключение с использованием учетных данных или сертификата пользователя;
- Асимметричное шифрование по открытому и закрытому ключу;
- Организация защищенного канала связи в распределенных системах даже в условиях открытой сети.

IntegrityGuard – плата аппаратного контроля состояния ПК

Назначение:
Отслеживание показаний состояния ПК

Основные функции

- аппаратный контроль температур и параметров микроклимата в корпусе ПК;
- обнаружение ударов и вибраций корпуса ПК;
- обнаружение вскрытия ПК.

Особенности

- исполнение для подключения в порт PCI Express и в формате 2,5-дюймового SATA-диска;
- подключение до 2 дополнительных датчиков 1-wire;
- подключение до 4 датчиков (сухой контакт);
- администрирование платы через физические ключи iButton;
- работа до 48 часов без питания с сохранением всего функционала, загрузка истроии событий при подключении питания;
- виджет для интеграции в систему визуализации Integrity SCADA.

scadaint.ru

634000, Россия, Томск,
ул. Алтайская, 161А
тел.: +7 (3822) 601-000, 499-200
e-mail: int@scadaint.ru
elesy@elesy.ru

ОБЕСПЕЧИВАЕТ ЗАЩИТУ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ОТ УГРОЗ БЕЗОПАСНОСТИ

УБИ.006 Угроза внедрения кода или данных;
УБИ.007 Угроза воздействия на программы с высокими привилегиями;
УБИ.028 Угроза использования альтернативных путей доступа к ресурсам;
УБИ.030 Угроза использования информации идентификации/аутентификации, заданной по умолчанию;
УБИ.031 Угроза использования механизмов авторизации для повышения привилегий;
УБИ.036 Угроза исследования механизмов работы программы;
УБИ.037 Угроза исследования приложения через отчеты об ошибках;
УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией;
УБИ.068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;
УБИ.069 Угроза неправомерных действий в каналах связи;
УБИ.074 Угроза несанкционированного доступа к аутентификационной информации;
УБИ.080 Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети;
УБИ.086 Угроза несанкционированного изменения аутентификационной информации;
УБИ.090 Угроза несанкционированного создания учетной записи пользователя;
УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации;
УБИ.121 Угроза повреждения системного реестра;
УБИ.122 Угроза повышения привилегий;
УБИ.128 Угроза подмены доверенного пользователя;
УБИ.152 Угроза удаления аутентификационной информации;
УБИ.156 Угроза утраты носителей информации;
УБИ.157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;
УБИ.158 Угроза форматирования носителей информации;
УБИ.185 Угроза несанкционированного изменения параметров настройки средств защиты информации;
УБИ.187 Угроза несанкционированного воздействия на средство защиты информации;
УБИ.188 Угроза подмены программного обеспечения;
УБИ.191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения.

634000, Россия, Томск,
ул. Алтайская, 161А
тел.: +7 (3822) 601-000, 499-200
e-mail: int@scadaint.ru
elesy@elesy.ru