kaspersky

Электронный блок управления SystemeLogic X для силовых автоматических выключателей SystemePact: отчет об оценке зрелости безопасности

#2024-0002-0003-EXT

Kaspersky ICS CERT

15.04.2024

kaspersky

kaspersky

Список сокращений

Сокращение	Значение
ACB	Air circuit breaker
ARM	Arm Holdings plc
CVSS	Common vulnerability scoring system
ICS CERT	Industrial control systems cyber emergency response team
IEEE	Institute of Electrical and Electronics Engineers
ISO	International standardization organization
IT	Information technology
MODBUS	Коммуникационный протокол прикладного уровня, предложенный Modicon (теперь Schneider Electric)
OT	Operational technology
PSIRT	Product security incident response team
RSS	RDF Site Summary / Really Simple Syndication
RTU	Remote telecommunication unit
SMM	Security maturity model, модель зрелости безопасности
USB	Universal serial bus
АО	Акционерное общество
АСУ	Автоматизированная система управления

АСУ ТП	Автоматизированная система управления технологическим процессом
БДУ	База данных угроз
БПО	Безопасное программное обеспечение
ИБ	Информационная безопасность
ИКТ	Информационно-коммуникационная инфраструктура
ИС	Информационная система
ИТ	Информационная технология
КД	Конструкторская документация
КИИ	Критическая информационная инфраструктура
МЭК	Международная электротехническая комиссия
НДВ	Недекларированные возможности
ООО	Общество с ограниченной ответственностью
ПО	Программное обеспечение
ФСТЭК	Федеральная служба по техническому и экспортному контролю

kaspersky

О проведении оценки зрелости безопасности

Данный документ представляет собой детальный отчёт о результатах проведения оценки зрелости безопасности для электронного блока управления SystemeLogic X для силовых автоматических выключателей SystemePact.

Оценка зрелости проводилась на основе Модели зрелости безопасности (IoT Security Maturity Model, IoT SMM), разработанной Консорциумом промышленного интернета вещей (Industry IoT Consortium). При оценке принимался во внимание *Целевой профиль зрелости безопасности*, который был разработан ранее для электронного блока управления SystemeLogicX и доступен по ссылке https://kas.pr/y523.

Отчёт подготовлен специалистами Kaspersky ICS CERT.

Объект оценки

Объектом данной оценки является электронный блок управления SystemeLogic X для силовых автоматических выключателей SystemePact следующих типоразмеров:

- SystemePact ACB1 на токи 400-1600A;
- SystemePact ACB2 на токи 800-4000A.

Блок управления выполнен на базе микроконтроллера AT32F437 с вычислительным ядром ARM Cortex-M4.

Основными функциями электронного блока управления являются:

- анализ работы электроустановки и выявление аварийных режимов в электрической сети;
- отключение коммутационного аппарата при обнаружении аварийного режима.

Вспомогательными функциями электронного блока управления являются:

- управление коммутационным аппаратом по месту установки и дистанционно;
- передача статусных сигналов и измеренных значений в вышестоящую систему управления;
- осциллографирование аварийных режимов.

Электронный блок управления SystemeLogic X допускает удаленное и местное наблюдение и управление функционированием автоматического выключателя. Устройство имеет следующие цифровые интерфейсы:

- RS-485 (Modbus RTU) и МЭК 60870-5-101 – для организации шинной системы связи между устройствами и/или организации канала связи с системами управления, например системами диспетчерского контроля и сбора данных;
- USB – для обслуживания и конфигурирования устройства посредством подключения сервисного ноутбука с предустановленными операционной системой Windows и специализированным ПО «Конфигуратор МТ».

В дальнейшем возможно расширение номенклатуры цифровых интерфейсов и добавление беспроводных способов связи с устройством посредством Bluetooth и NFC.

Общий вид лицевой панели электронного блока управления SystemeLogic X представлен на рис. 1.

Светодиоды	Описание
Ready	Готовность устройства к работе
	Состояние устройства (необходимость ремонта).
	Сигнализация перегрузки
Ir	Срабатывание защиты от перегрузки
Isd Ii	Срабатывание селективной или мгновенной отсечки
Ig IΔn	Срабатывание защиты от замыкания на землю или дифференциальной защиты
Op.	Срабатывание дополнительных защит
Rx Tx	Работа коммуникационного порта

Рис. 1. Общий вид лицевой панели электронного блока управления SystemeLogic X для силовых автоматических выключателей SystemePact.

Цель оценки зрелости безопасности

С появлением в системах энергоснабжения промышленных предприятий, установок и офисных зданий цифровых устройств с функциями удалённого управления и мониторинга автоматических выключателей, электрические цепи больше не могут считаться инфраструктурным сегментом, изолированным от кибератак. Блоки управления автоматическими выключателями интегрируются в

системы диспетчеризации электроснабжения и решают задачи обеспечения киберфизических промышленных систем бесперебойным электропитанием с заданными параметрами и защиты промышленного оборудования от токов перегрузки и короткого замыкания.

Успешно проведенная атака на устройство может вызвать утечку данных, потерю данных, простой, сбой процесса распределения электроэнергии, нарушение функционирования промышленных и социальных объектов, в том числе критической инфраструктуры, в некоторых случаях повлечь за собой ущерб здоровью и жизни людей или экологический ущерб. Последствия атаки могут иметь негативный эффект в том числе для производителя устройств, который выражается в репутационных рисках, потере клиентов, финансовых потерях и снижении объема продаж.

Разработчик электронных блоков управления SystemeLogic X силовыми автоматическими выключателями SystemePact хочет удостовериться, что функционал устройства, равно как и процессы управления уязвимостями защищены в достаточной мере, чтобы обеспечить в долгосрочной перспективе кибербезопасность систем диспетчеризации электроэнергии, промышленных объектов и установок.

Целью оценки уровня зрелости безопасности и повышения защищённости является поддержка эффективного, а не избыточного и произвольного, использования механизмов защиты. Для оценки одновременно применяются показатели полноты и специфичности реализации требований безопасности[1] с одновременным учетом стоимости этой реализации.

Полнота реализации рассматривает глубину проработки и внимание к деталям реализации требований безопасности, повышая общие гарантии защиты устройства и его окружения, а **специфичность** учитывает отраслевые требования и другие специальные условия и ограничения реализации безопасности со стороны применения системы.

Задачей оценки уровня зрелости безопасности является оценка полноты и специфичности требований безопасности для процессов разработки, использования и обслуживания устройства. Целевые уровни показателей полноты и специфичности для требований (практик) безопасности задокументированы в разработанном для устройства *Целевом профиле зрелости безопасности*.

Целевой профиль зрелости безопасности устанавливает необходимый и достаточный уровень зрелости безопасности для рассматриваемого устройства. Целевой профиль состоит из перечня практик безопасности с их уровнями

[1] Полнота реализации требований безопасности далее указывается как «полнота». Специфичность реализации требований безопасности далее указывается как «специфичность».

полноты и специфичности реализации, которые дают заинтересованным сторонам проекта понимание целей безопасности и задач каждой практики безопасности.

Метод оценки зрелости безопасности

Оценка текущего состояния зрелости безопасности проводилась посредством интервьюирования сотрудников АО «Систэм Электрик», анализа пользовательской документации и документации по обеспечению безопасности, а также на основании результатов поиска и оценки уязвимостей в реализации логических протоколов MODBUS RTU и МЭК-60870-5-101.

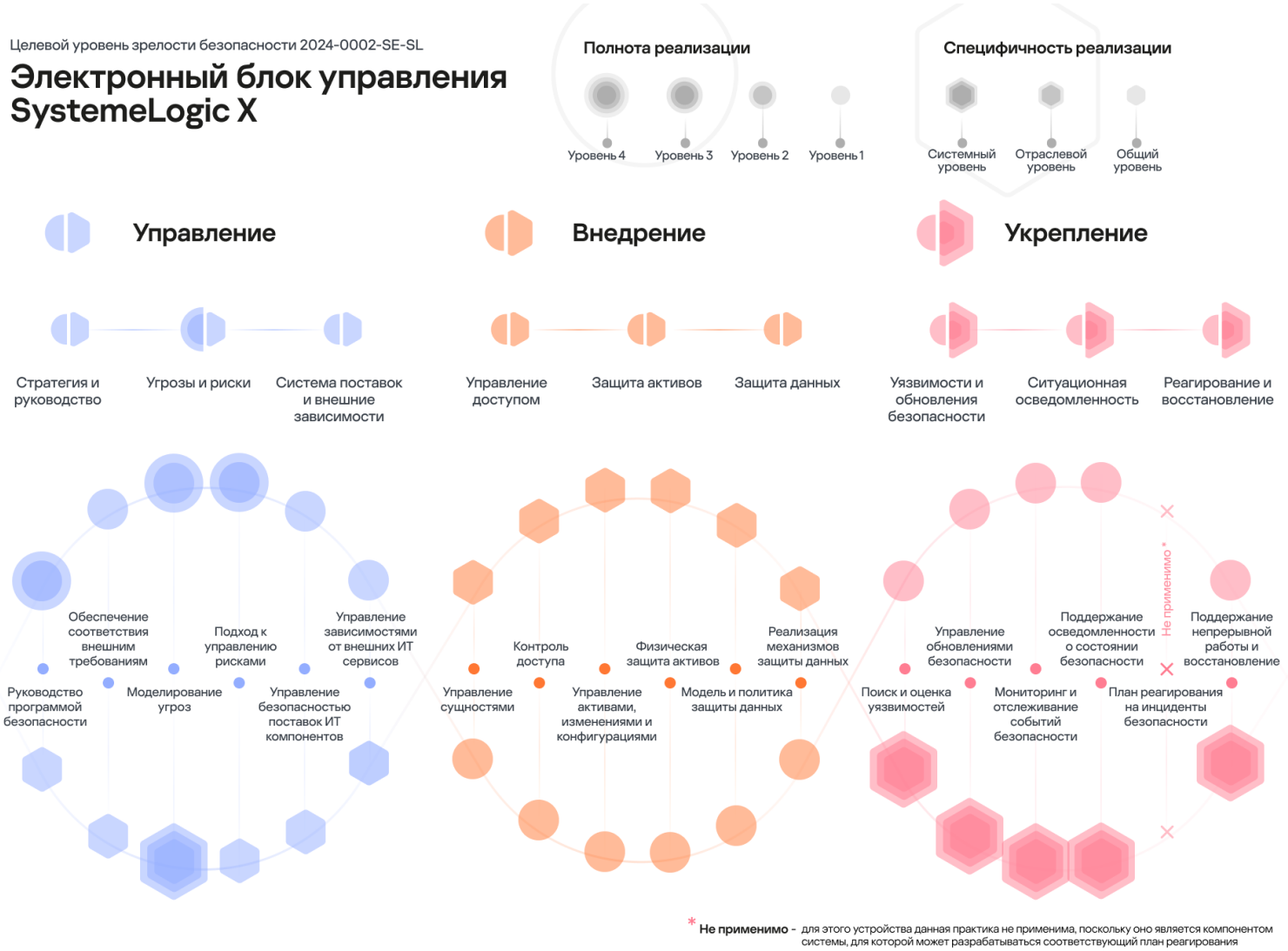
Интервьюирование сотрудников проводилось в два этапа:

- Первый этап заключался в заполнении опросника, вопросы которого не были сопоставлены с конкретными практиками безопасности и уровнями полноты их реализации, чтобы избежать предвзятости в ответах;
- Второй этап стартовал после обработки результатов первого этапа. На данном этапе были представлены предварительные результаты оценки полноты практик безопасности. Затем, для устранения противоречий, полученных на первом этапе, для восполнения пробелов в данных и, где необходимо, для предоставления свидетельств, подтверждающих ранее данные ответы, был использован дополнительный опросник. Также на данном этапе проводилась оценка уровня специфичности практик (общий, отраслевой или системный).

Оценка уязвимостей, которая проводилась как отдельная и независимая процедура, позволила получить информацию, насколько заявленные уровни полноты практик соотносятся с реальной технической реализацией этих практик.

Результаты интервьюирования и анализа свидетельств, пользовательской документации, документации по обеспечению безопасности, а также Отчет о проверке на уязвимости (Приложение #1 к данному документу) позволили сделать заключение о соответствии объектов оценки заявленному Целевому профилю зрелости безопасности.

Целевой уровень зрелости безопасности



kaspersky

Результаты оценки зрелости безопасности

Практика безопасности	Целевая полнота	Уровень полноты	Целевая специфичность	Уровень специфичности
Руководство программой безопасности	2 / Ситуативный	2 / Ситуативный	Общий	Общий
Обеспечение соответствия внешним требованиям	1 / Минимальный	1 / Минимальный	Общий	Общий
Моделирование угроз	2 / Ситуативный	2 / Ситуативный	Системный	Системный
Подход к управлению рисками	2 / Ситуативный	2 / Ситуативный	Общий	Общий
Управление безопасностью поставок ИТ компонентов	1 / Минимальный	1 / Минимальный	Общий	Общий
Управление зависимостями от внешних ИТ сервисов	1 / Минимальный	1 / Минимальный	Общий	Общий
Управление сущностями	1 / Минимальный	1 / Минимальный	Общий	Общий
Контроль доступа	1 / Минимальный	1 / Минимальный	Общий	Общий

Управление активами, изменениями и конфигурацией	**1 / Минимальный**	**1 / Минимальный**	**Общий**	**Общий**
Физическая защита активов	**1 / Минимальный**	**1 / Минимальный**	**Общий**	**Общий**
Модель и политика для данных	**1 / Минимальный**	**1 / Минимальный**	**Общий**	**Общий**
Реализация механизмов защиты данных	**1 / Минимальный**	**1 / Минимальный**	**Общий**	**Общий**
Поиск и оценка уязвимостей	**1 / Минимальный**	**1 / Минимальный**	**Системный**	**Системный**
Управление обновлениями безопасности	**1 / Минимальный**	**1 / Минимальный**	**Системный**	**Системный**
Мониторинг и отслеживание событий безопасности	**1 / Минимальный**	**1 / Минимальный**	**Системный**	**Системный**
Поддержание осведомлённости о состоянии безопасности	**1 / Минимальный**	**1 / Минимальный**	**Системный**	**Системный**
План реагирования на инциденты безопасности	–	–	–	–
Поддержание непрерывной работы и восстановление	**1 / Минимальный**	**1 / Минимальный**	**Системный**	**Системный**

Руководство программой безопасности

Уровни полноты и специфичности	
	2 / Ситуативный **Общий**
Цели безопасности	
	Систэм Электрик стремится создать программу безопасности, исходя из своей организационной структуры и номенклатуры выпускаемых цифровых устройств.
Заключение	
	В целом компания демонстрирует надлежащий подход к внедрению общих практик управления кибербезопасностью и безопасной разработки устройства. Для обеспечения данных практик в компании выделены штатные единицы, в соответствии с внутренними документами сотрудники компании обязаны проходить обучение в области обеспечения кибербезопасности. Требования кибербезопасности для устройства задокументированы и отслеживаются в процессе разработки. **Руководство программой безопасности соответствует уровню полноты 2 / Ситуативный.** **Уровень специфичности – Общий.**

kaspersky

Обеспечение соответствия внешним требованиям

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	Систэм Электрик осознаёт необходимость соответствия внешним требованиям, предъявляемым к устройству.
Заключение	
	Обеспечивается соответствие общим требованиям безопасности, предъявляемым заказчиками. Компания Систэм Электрик демонстрирует понимание, что устройство может быть частью объекта КИИ, что может послужить источником дополнительных требований к устройству. **Обеспечение соответствия внешним требованиям соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Моделирование угроз

Уровни полноты и специфичности	
	2 / Ситуативный **Системный**
Цели безопасности	
	Систэм Электрик проводит анализ уязвимостей для идентификации угроз. При анализе обнаруженных угрозы используется ситуативный подход.
Заключение	
	Систэм Электрик рассматривает угрозы кибербезопасности, характерные для данного класса устройств. При анализе угроз используются общедоступные инструменты. Для каждой угрозы определяется вероятность реализации и критичность последствий. **Моделирование угроз соответствует уровню полноты 2 / Ситуативный.** **Уровень специфичности – Системный.**

kaspersky

Подход к управлению рисками

Уровни полноты и специфичности	
	2 / Ситуативный **Общий**
Цели безопасности	
	Систэм Электрик поддерживает процедуры детальной оценки рисков с их ранжированием в зависимости от степени критичности.
Заключение	
	Систэм Электрик проводит и документирует оценку рисков, используя ситуативный подход. **Подход к управлению рисками соответствует уровню полноты 2 / Ситуативный.** **Уровень специфичности – Общий.**

kaspersky

Управление безопасностью поставок ИТ компонентов

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	Систэм Электрик разработала процедуры проверки подлинности поставщиков и поставляемых компонентов, а также отслеживает исполнение данных процедур.
Заключение	
	ПО устройства содержит сторонние компоненты с открытым исходным кодом. В Систэм Электрик прописаны и реализованы основные процедуры по снижению рисков кибербезопасности, связанными с данными компонентами. **Управление безопасностью поставок ИТ компонентов соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Управление зависимостями от внешних ИТ сервисов

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	Систэм Электрик стремится отслеживать репутацию поставщиков внешних ИТ сервисов и заключает с ними типовые соглашения.
Заключение	
	Систэм Электрик заключает с поставщиками договоры о конфиденциальности и безопасности сторонних ИТ сервисов. Сотрудники компании проходят обучение по правилам безопасного использования внешних сервисов. **Управление зависимостью от внешних ИТ сервисов соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Управление сущностями

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	В электронном блоке управления реализован базовый функционал идентификации устройства и пользователей.
Заключение	
	Электронный блок управления однозначно идентифицируется по заводскому номеру. Для заказчика предусмотрено две роли, при помощи которых можно организовать управление доступом: «Гость» и «Инженер». **Управление сущностями соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Контроль доступа

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	Электронный блок управления ограничивает доступ внешних субъектов.
Заключение	
	В устройстве реализованы базовые механизмы разграничения и контроля доступа на основе двух ролей – «Гость» и «Инженер». Без авторизации возможен лишь доступ на считывание параметров устройства, расширенные права по управлению и конфигурированию устройства доступны только после авторизации под ролью «Инженер». **Контроль доступа соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Управление активами, изменениями и конфигурацией

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	Систэм Электрик разработала процедуры управления конфигурацией и изменениями для производимых устройств.
Заключение	
	Эксплуатационная документация для электронного блока управления содержит рекомендации по первоначальной конфигурации и обеспечению кибербезопасности устройства. **Управление активами, изменениями и конфигурацией соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Физическая защита активов

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	Систэм Электрик предоставила общие рекомендации по ограничению физического доступа к устройству.
Заключение	
	В эксплуатационной документации приведены базовые рекомендации по ограничению физического доступа к устройству со стороны неавторизованного персонала. **Физическая защита активов соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Модель и политика защиты данных

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	Систэм Электрик разработала процедуры проверки подлинности поставщиков и поставляемых компонентов, а также отслеживает исполнение данных процедур. Declare that IT and OT data should be protected from unauthorized access.
Заключение	
	Для электронного блока управления определены типы защищаемых данных и общие меры по их защите. **Модель и политика защиты данных соответствуют уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Реализация механизмов защиты данных

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели безопасности	
	Для защиты данных используются встроенные в электронный блок управления механизмы контроля.
Заключение	
	В электронном блоке управления реализованы базовые механизмы защиты данных. В эксплуатационной документации даны дополнительные рекомендации по защите на стороне заказчика. **Реализация механизмов защиты данных соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Поиск и оценка уязвимостей

Уровни полноты и специфичности	
	1 / Минимальный **Системный**
Цели безопасности	
	Систэм Электрик проводит оценку известных уязвимостей, обнаруженных в активах компании.
Заключение	
	В Систэм Электрик реализованы типовые процессы поиска и оценки уязвимостей для ИКТ-инфраструктуры и компонентов устройства. **Поиск и оценка уязвимостей соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Системный.**

kaspersky

Управление обновлениями безопасности

Уровни полноты и специфичности	
	1 / Минимальный **Системный**
Цели безопасности	
	Систэм Электрик следует рекомендациям по кибербезопасности от разработчиков сторонних компонентов ПО.
Заключение	
	В Систэм Электрик внедрены базовые процедуры управления обновлениями компонентов ПО устройства и инструментов разработки. Загрузка обновлённой прошивки в электронный блок управления осуществляется силами Систэм Электрик в рамках сервисного обслуживания. **Управление обновлениями безопасности соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Системный.**

Мониторинг и отслеживание событий безопасности

Уровни полноты и специфичности	
	1 / Минимальный **Системный**
Цели безопасности	
	Электронный блок управления должен обеспечивать возможность записи и чтения событий безопасности в журнал сообщений.
Заключение	
	Электронный блок управления реализует базовый функционал мониторинга событий безопасности. Журналируются события, связанные с конфигурированием, срабатыванием алгоритмов защиты и подсистемой безопасности устройства. **Мониторинг и отслеживание событий безопасности соответствуют уровню полноты 1 / Минимальный.** **Уровень специфичности – Системный.**

kaspersky

Поддержание осведомлённости о состоянии безопасности

Уровни полноты и специфичности	
	1 / Минимальный **Системный**
Цели безопасности	
	Систэм Электрик отслеживает внешние источники информации об инцидентах информационной безопасности, а также предоставляет заказчикам необходимую информацию, касающуюся безопасности электронного блока управления.
Заключение	
	Систэм Электрик отслеживает информацию об известных уязвимостях в компонентах устройства. Компания информирует заказчиков о необходимости замены и модернизации устройств, об обнаружении уязвимостей, а также о выходе обновлений и исправлений программной части электронного блока управления. **Поддержание осведомлённости о состоянии безопасности соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Системный.**

kaspersky

План реагирования на инциденты безопасности

Уровни полноты и специфичности	
	Данная практика не применима на уровне электронного блока управления. Устройство является составной частью системы управления энергопитанием, для которой разрабатываются планы реагирования на инциденты безопасности.

kaspersky

Поддержание непрерывной работы и восстановление

Уровни полноты и специфичности	
	1 / Минимальный **Системный**
Цели безопасности	
	Систэм Электрик предоставляет базовые рекомендации по восстановлению устройства.
Заключение	
	Замену, текущий ремонт и восстановление электронных блоков управления производит предприятие, обеспечивающее гарантийное и послегарантийное обслуживание. **Поддержание непрерывной работы и восстановление соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Системный.**

www.kaspersky.ru/

https://ics-cert.kaspersky.ru/