kaspersky

Электронный блок управления SystemeLogicX для силовых автоматических выключателей SystemePact: целевой профиль зрелости безопасности #2024-0002-SE-SL

ICS CERT
Kaspersky

13.03.2024

kaspersky

Содержание

kaspersky

Введение

Задача данного документа – описать целевой уровень зрелости безопасности для электронного блока управления Systeme Logic X силовых автоматических выключателей SystemePact, разработанных АО «Систэм Электрик» в соответствии с Моделью зрелости безопасности интернета вещей.

Целевой уровень определяется производителем до проведения внешней оценки функций безопасности, их полноты и соответствия типу устройства, а также до любого дальнейшего улучшения соответствующих функций безопасности.

Описание метода оценки зрелости безопасности

Оценка зрелости безопасности проводится как отдельная и независимая процедура, которая позволяет определить, насколько заявленные уровни полноты практик безопасности соотносятся с реальной технической реализацией мер защиты и процессами обеспечения безопасности.

Модель зрелости безопасности, разработанная Индустриальным консорциумом интернета вещей, определяет уровни зрелости практик безопасности для устройства в контексте сценариев его применения и присущих ему рисков кибербезопасности. Это позволяет ответственным лицам в области кибербезопасности инвестировать имеющиеся ресурсы только в механизмы обеспечения безопасности, соответствующие конкретным требованиям организации.

Задача модели зрелости безопасности – определить целевой (требуемый) уровень зрелости безопасности для устройства и очередность действий, необходимых для его достижения.

Модель способствует эффективному и продуктивному взаимодействию между руководителями организации и техническими специалистами. Руководители организации, менеджеры по бизнес-рискам и владельцы промышленных систем, заинтересованные в правильной стратегии внедрения практик обеспечения безопасности, могут сотрудничать с аналитиками, архитекторами, разработчиками, системными интеграторами и другими лицами, ответственными за техническую реализацию.

Иерархия практик зрелости безопасности

Ядро модели зрелости безопасности представлено иерархией практик обеспечения безопасности. На рисунке 1 показана модель зрелости безопасности с разбивкой по доменам, поддоменам и отдельным практикам.

Рис. 1. Иерархия модели зрелости безопасности: домены, поддомены и практики безопасности

Домены представляют верхний уровень модели, охватывающий ключевые аспекты зрелости безопасности: «Управление», «Внедрение» и «Укрепление».

Каждый домен разделен на несколько поддоменов – ключевых групп, соответствующих аспектам безопасности. Например, в домен «Укрепление» входят такие поддомены, как «Уязвимости и обновления безопасности», «Ситуационная осведомленность» и «Реагирование и восстановление». В свою очередь, в каждом поддомене для достижения определенных результатов могут использоваться практики как технического, так и организационного характера.

Такой иерархический подход позволяет анализировать расхождение текущего и целевого уровней зрелости с разной степенью детализации, от уровня доменов до отдельных практик.

Домены играют ключевую роль при определении приоритетов направлений развития безопасности на стратегическом уровне. На уровне доменов ответственное лицо определяет приоритет направлений развития безопасности.

Поддомены отображают базовые способы регулирования этих приоритетов на уровне планирования. На уровне поддоменов ответственное лицо выявляет основные потребности, чтобы переадресовать их для решения задач безопасности.

Практики представляют собой стандартные мероприятия, связанные с поддоменами и определяемые на тактическом уровне. На уровне практик ответственное лицо рассматривает необходимость конкретных мероприятий по обеспечению безопасности.

Целевой уровень зрелости безопасности

Целью оценки и повышения уровня зрелости безопасности является обеспечение эффективности, а не произвольное применение механизмов безопасности. При таком подходе определяется соотношение полноты (степени глубины, единства подхода и эффективности мер безопасности) и специфичности (степени соответствия отраслевым и системным задачам) требований к безопасности с инвестициями имеющихся ресурсов в соответствующие практики.

Целевой уровень зрелости безопасности определяется совокупным набором практик обеспечения безопасности с требующимися уровнями полноты и специфичности, который представляет всем заинтересованным лицам понимание как общих целей безопасности, так и назначения каждой конкретной практики безопасности.

Задача определения целевого уровня зрелости безопасности ложится на плечи заинтересованных лиц со стороны бизнес-подразделений и должна быть выполнена прежде выполнения каких-либо мероприятий по повышению уровня безопасности.

Определение целевого уровня зрелости безопасности

Объект оценки и предполагаемые сценарии его использования

Описание объекта оценки

Объектом оценки является электронный блок управления SystemeLogic X для силовых автоматических выключателей SystemePact (далее – «Объект защиты» или «ОЗ»), построенный 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.

Электронные блоки управления SystemeLogic X допускают 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. 2.

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

Предполагаемые сценарии использования

Автоматические выключатели с электронным блоком управления SystemeLogic X применяются в распределительных устройствах низкого напряжения (РУНН) 0,4 – 0,6 кВ для защиты электрических цепей промышленных объектов от перегрузок и токов короткого замыкания. Устройство обеспечивает:

- электроснабжение надлежащего качества;
- безопасность персонала, электросетей и промышленных установок посредством защиты:
  - от перегрузок;
  - от короткого замыкания;
  - от замыканий на землю;
  - от утечек на землю;
  - нейтрали;
- селективность при последовательном соединении нескольких устройств для быстрого отключения части электросети, где возникла нештатная ситуация, и сохранения подачи питания в остальную часть сети;
- измерение значений токов, напряжений, мощности и энергии, частот и коэффициентов гармонических искажений;
- проверку состояния и диагностику отдельных функций устройства;
- возможность конфигурирования непосредственно по месту нахождения устройства через USB и ПО «Конфигуратор МТ»;
- регистрацию событий, связанных с режимом работы, обслуживанием и настройкой устройства.

kaspersky

Предпосылки и контекст безопасности

Область применения

АО «Систэм Электрик» — российский производитель оборудования и разработчик комплексных решений для проектов по передаче и распределению электроэнергии.

Рассматриваемые блоки управления и автоматические выключатели принадлежат к распространенному классу коммутационного оборудования, используемого для построения промышленных электрических цепей и энергетических систем.

Устройства должны обеспечивать безопасность персонала и защиту электрических цепей промышленных объектов от перегрузок и токов короткого замыкания, а также измерение параметров сети и регистрацию событий, связанных с их эксплуатацией, безопасностью или нештатными ситуациями.

Устройства, производимые АО «Систэм Электрик», изготавливаются на следующих производственных площадках:

- завод «Потенциал» в республике Марий Эл;
- завод «ЭлектроМоноблок» («СЭЗЭМ») в Ленинградской области;
- НТЦ «Механотроника» в Санкт-Петербурге (для оцениваемого устройства);
- производственные площадки поставщиков компонентов.

Устройства монтируются в распределительных шкафах, являющихся частью инфраструктуры промышленной установки или площадки. Ввиду разнообразия климатических условий на различных площадках, при монтаже должны обеспечиваться показатели температуры, влажности, запыленности и механических воздействий, рекомендуемые производителем для устанавливаемых моделей устройств.

Для удобства регистрации показателей, настройки и управления, устройства интегрируются в цифровую инфраструктуру предприятия, цеха или промышленной установки.

В общем случае, в среде функционирования к устройству имеет доступ следующие категории персонала:

- персонал эксплуатирующей организации (оператора);
- персонал подрядных организаций (монтажных, наладочных);
- иной персонал, которому на временной или постоянной основе предоставлен доступ к устройству или смежным с ним системам.

В среде разработки к устройству имеет доступ инженерный и административной персонал Systeme Electric и предприятия-изготовителя (НТЦ «Механотроника»).

Подверженность атакам

Кибератаки могут осуществляться как посредством физического доступа к панели управления, USB-порту или разъему RS-485, так и проводиться удалённо, если устройство подключено к ТСПД предприятия, например - посылкой управляющих команд из скомпрометированной системы диспетчерского контроля.

Для атаки на устройство может использоваться легитимные или модифицированные версии ПО «Конфигуратор МТ».

Устройства могут как быть конечной целью кибератаки, так и являться инструментами в цепочке проведения атаки, когда целью нарушителя является компрометация процесса распределения электроэнергии или части инфраструктуры объекта энергоснабжения.

kaspersky

Ландшафт угроз

Согласно отчёту Kaspersky ICS CERT о ландшафте угроз для систем промышленной автоматизации, во втором полугодии 2023 г. для промышленных сетей основными источниками распространения вредоносного кода остаются Интернет, почтовые клиенты и съемные носители.

Согласно тому же отчету, в системах промышленной автоматизации наиболее часто выявлялась активность следующих вредоносных объектов:

- вредоносные скрипты и фишинговые страницы;
- ресурсы в сети Интернет из списка запрещённых;
- троянские программы, бэкдоры и кейлоггеры;
- вредоносные документы форматов MSOffice и PDF;
- черви и вирусы.

Источниками угроз для ОЗ выступают виды нарушителей, общие для систем промышленной автоматизации (в зависимости от объекта применения ОЗ): от спецслужб иностранных государств, террористических и криминальных групп до работников предприятия и внешних подрядчиков.[1]

Ноутбуки и компьютеры диспетчеров и инженеров, системных и сетевых администраторов, разработчиков, интеграторов и подрядчиков имеют сопряжение одновременно с ТСПД и с КСПД. Компьютеры, ноутбуки и USB-модемы могут реализовывать несанкционированный канал доступа в Интернет или недоверенную сеть (например, в инфраструктуру интегратора или подрядчика). Учётные записи указанных групп пользователей, как правило, имеют широкие полномочия по настройке и конфигурированию устройств ТСПД, что делает данные учетные записи привлекательной целью для атак злоумышленников.

Актуальность

Автоматические выключатели широко применяются для построения электрических сетей промышленных установок и предприятий. Перед данным типом устройств ставятся задачи обеспечения киберфизических промышленных систем бесперебойным электропитанием с заданными параметрами и защита электроцепей и промышленного оборудования от токов перегрузки и короткого замыкания.

Следующие рекомендации могут применяться для обеспечения кибербезопасности устройства на этапах разработки, производства и эксплуатации:

- ГОСТ Р 56939-2016 «Разработка безопасного программного обеспечения. Общие требования»;
- IEC 62443-4-1-2018 “Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements”;
- ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- ГОСТ Р ИСО/МЭК 27019-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике (неатомной)».

Применимость конкретных практик безопасности определяется спецификой организации и инфраструктуры конкретного промышленного объекта и условиями применения устройства в этой инфраструктуре.

Релевантность

Изначально электрические цепи являлись достаточно изолированным инфраструктурным сегментом, однако внедрение в них цифровых устройств с функциями удаленного управления, мониторинга,

[1] Характеристики источника угроз

подключения и взаимодействия с другими цифровыми устройствами, существенно увеличивают поверхность атаки.

Безотлагательность

В электронных компонентах и прошивках цифровых устройств электрических сетей могут присутствовать уязвимости. Процедуры предоставления и контроля физического доступа к месту установки устройства могут быть не определены или не выполняться должным образом.

Используя имеющиеся уязвимости и несовершенство процедур управления доступом, злоумышленники могут вызвать нарушение функционирования или ложное срабатывание устройства, заменить прошивку или часть кода устройства.

С точки зрения кибербезопасности, технологии и сервисы, предназначенные для доступа и управления устройствами, равно как и функции мониторинга состояния устройства, а также процессы управления уязвимостями и обновлениями безопасности, требуют первоочередного и неотложного внимания со стороны производителя устройства.

Ущерб от угроз

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.

Сложности и ограничения

Требования по обеспечению кибербезопасности не должны негативно сказываться на функциональной безопасности устройства. Так, из-за специфики применения устройства не поддерживается регулярная автоматическая установка обновлений безопасности. Требования кибербезопасности должны быть органично интегрированы в этапы проектирования, разработки и производства.

Кроме того, микроконтроллерная архитектура и невысокая вычислительная мощность компонентов устройства налагают существенные ограничения на реализацию необходимых функций кибербезопасности, таких как, например, мониторинг событий, защита данных, контроль и организация доступа.

С другой стороны, в текущей версии устройства отсутствуют аппаратные компоненты, отвечающие за функции беспроводной связи с устройством по Bluetooth и NFC, что уменьшает потенциальную поверхность атаки для злоумышленников.

Предпосылки доверия

Интерфейсы и конфигурация устройства, а также измеряемые и передаваемые им параметры электросети должны быть защищены надлежащим образом с применением организационных и технических мер защиты.

Функции безопасности устройства должны дополняться внешними наложенными решениями по обеспечению кибербезопасности на уровне промышленного предприятия. Безопасная работа устройства обеспечивается с учетом того, что все компоненты инфраструктуры промышленного объекта защищены должным образом.

Процедуры безопасной установки, эксплуатации и конфигурирования, равно как и перечень и обязанности лиц, имеющих доступ к устройству определяются в соответствии с политикой безопасности, принятой на промышленном объекте.

Распределение работ

Оценка соответствия реализованных мер кибербезопасности целевому уровню зрелости проводится в несколько этапов.

Первый этап, разработка Целевого профиля зрелости безопасности, предусматривает определение ответственными работниками Систэм Электрик высокоуровневых целей безопасности для ОЗ и необходимых уровней зрелости для отдельных практик безопасности. Данная информация заносится аналитиками Kaspersky в Целевой профиль, который валидируется и проходит согласование с представителями Систэм Электрик.

На втором этапе на основе целевого профиля аналитики Kaspersky готовят опросники для определения текущего состояния безопасности ОЗ. Оценка текущего состояния проводится посредством интервьюирования работников Систэм Электрик и анализа предоставленной документации и иных артефактов разработки и производства.

Одновременно со вторым этапом проводится третий этап, заключающийся в оценке командой исследователей Kaspersky безопасности устройства с использованием технических средств, поиске и оценке уязвимостей. Информация, полученная на данном этапе, также будет использована для определения текущего состояния безопасности устройства.

На четвертом этапе аналитики Kaspersky на основе полученных данных выявляют возможные отклонения от целевого уровня зрелости безопасности и готовят рекомендации по устранению несоответствий. Результирующими документами на этой стадии являются Отчёт о степени соответствия реализованных мер безопасности и Детальный технический отчёт о выявленных уязвимостях.

На завершающем этапе Kaspersky и Систэм Электрик согласуют и финализируют документы, разработанные на предыдущих этапах.

Ожидаемые результаты выполнения работ

В результате выполнения работ Kaspersky должен разработать и передать заказчику следующие отчётные документы:

- Целевой профиль зрелости безопасности;
- Требования к реализации практик безопасности на этапе разработки устройства;
- Детальный отчет об оценке зрелости безопасности;
- Отчет об оценке зрелости безопасности;
- Отчет о проверке на уязвимости (Приложение #1 к Детальному отчёту);
- Свидетельство об оценке соответствия целевому профилю зрелости безопасности (при условии достижения критериев положительной оценки).

Зависимости работ

Сроки выполнения работ по оценке текущего состояния в значительной степени зависят от объема документации, относящейся к обеспечению кибербезопасности компании Систэм Электрик, и своевременного представления работникам Kaspersky требуемых документации и свидетельств, а также доступности отдельных членов команды Систэм Электрик для участия в совещаниях. Необходимо учитывать данные обстоятельства при составлении и корректировке плана проектных активностей, чтобы исключить непредвиденные задержки при выполнении работ.

kaspersky

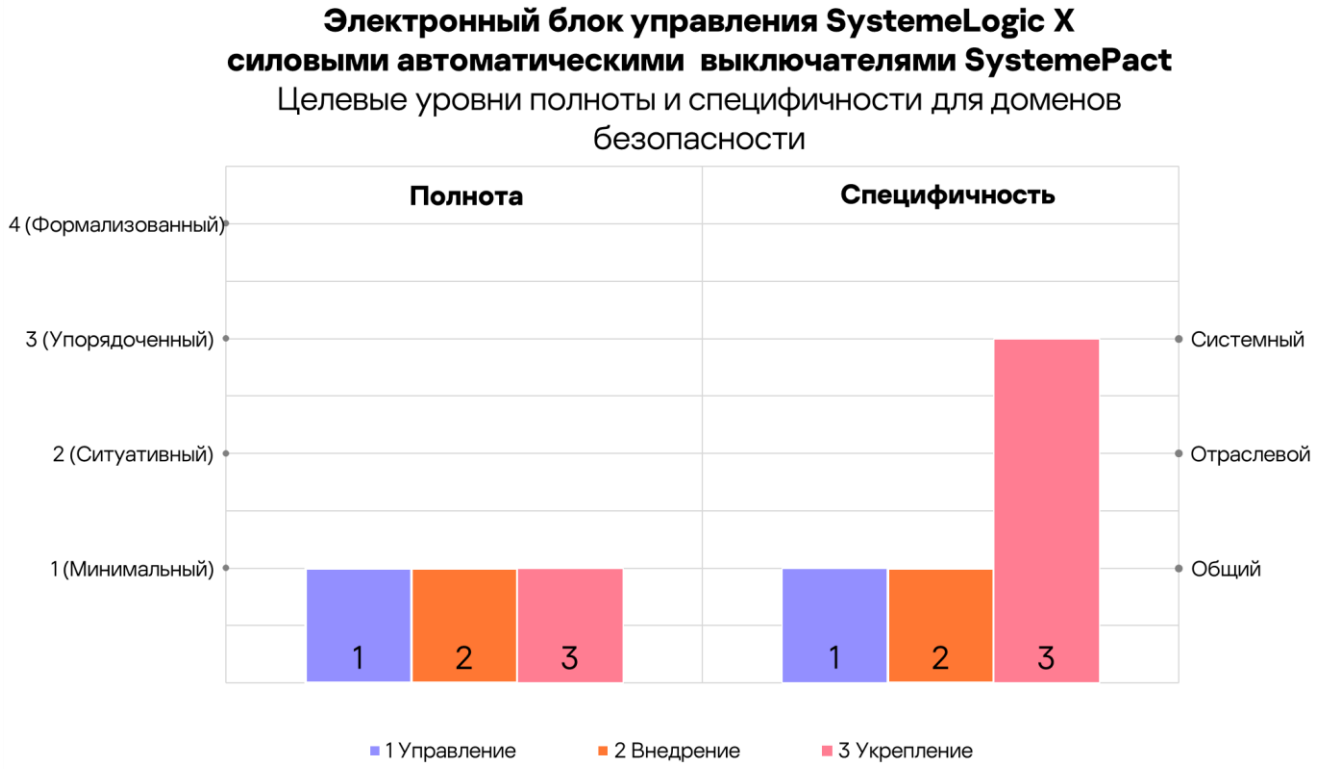
Описание необходимого уровня зрелости и оценка текущего состояния

В настоящем разделе приводятся результаты анализа приоритетов обеспечения безопасности в соответствии с контекстом, рассмотренным в предыдущем разделе. Целевые уровни полноты и специфичности раскрыты на каждом из трёх уровней Модели зрелости безопасности – на уровне отдельных доменов, поддоменов и практик. Результирующие целевые уровни полноты и специфичности провалидированы и проверены на непротиворечивость относительно реальных целей и потребностей по обеспечению безопасности.

Установка целей и приоритетов для доменов безопасности

На уровне доменов были определены следующие приоритетные направления обеспечения безопасности.

Установленные уровни полноты и специфичности доменов могут быть скорректированы на этапе валидации Целевого профиля для их согласования с соответствующими уровнями поддоменов безопасности.



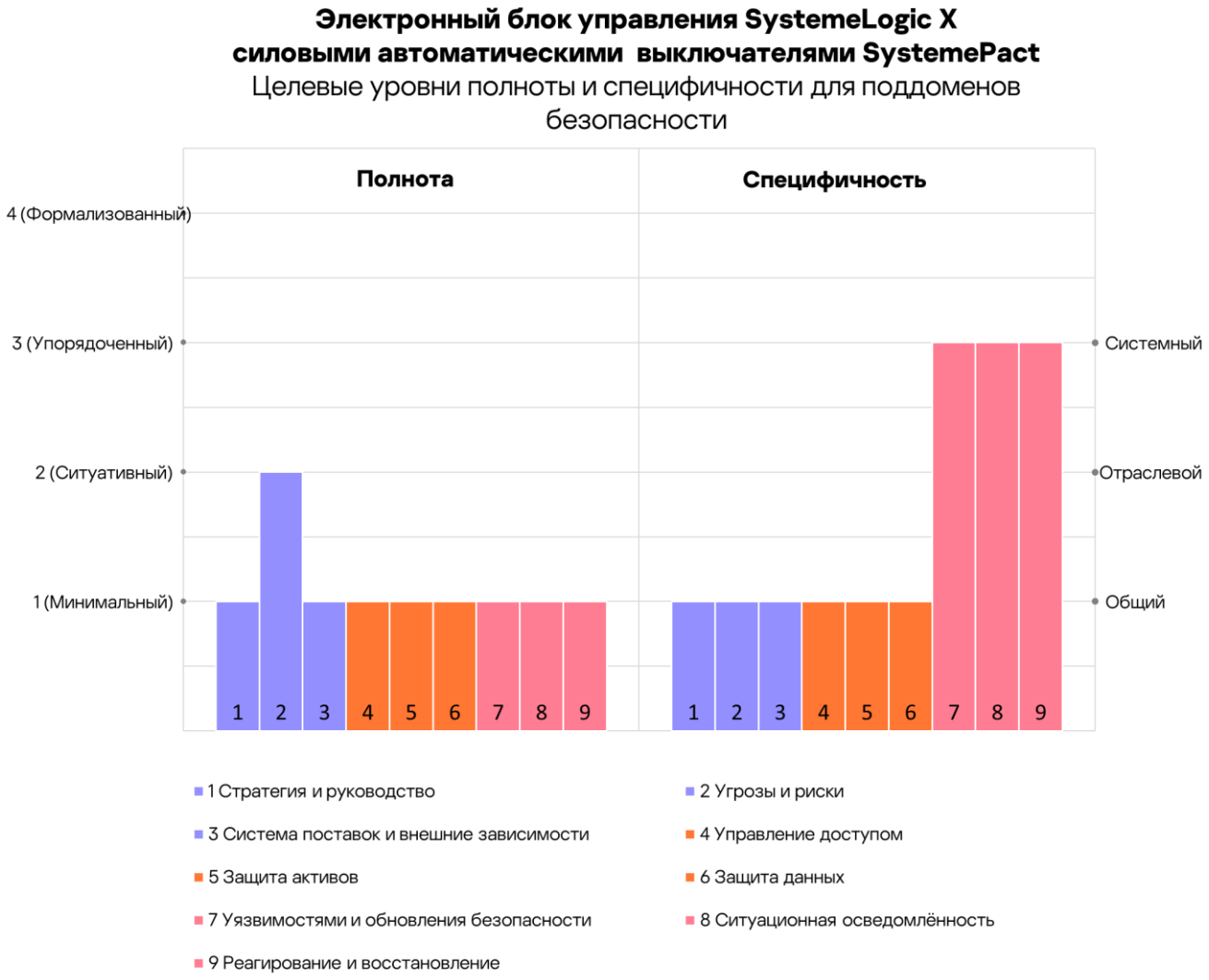
Домен безопасности	Цели и приоритеты домена	Уровень полноты	Уровень специфичности
Управление	Следование общим соображениям кибербезопасности устройства	**1 / Минимальный**	**1 / Общий**
Внедрение	Использование минимально необходимого перечня из общепринятых мер безопасности	**1 / Минимальный**	**1 / Общий**

Укрепление	Применение и рекомендации практик кибергигиены	**1 / Минимальный**	**3 / Системный** Операционные мероприятия по поддержанию состояния кибербезопасности устройства в значительно мере определяются спецификой (условиями) применения устройства, соответствующая информация отражена в описании уровня специфичности отдельных практик безопасности, относящихся к этому домену

Определение потребностей для поддоменов безопасности

Исходя из определения целей для доменов безопасности и соответствующих им уровней полноты и специфичности, устанавливаются и корректируются целевые потребности для поддоменов.

Установленные уровни полноты и специфичности поддоменов могут быть скорректированы на этапе валидации Целевого профиля для их согласования с соответствующими уровнями практик безопасности, адаптированными под специфику и условия использования устройства.



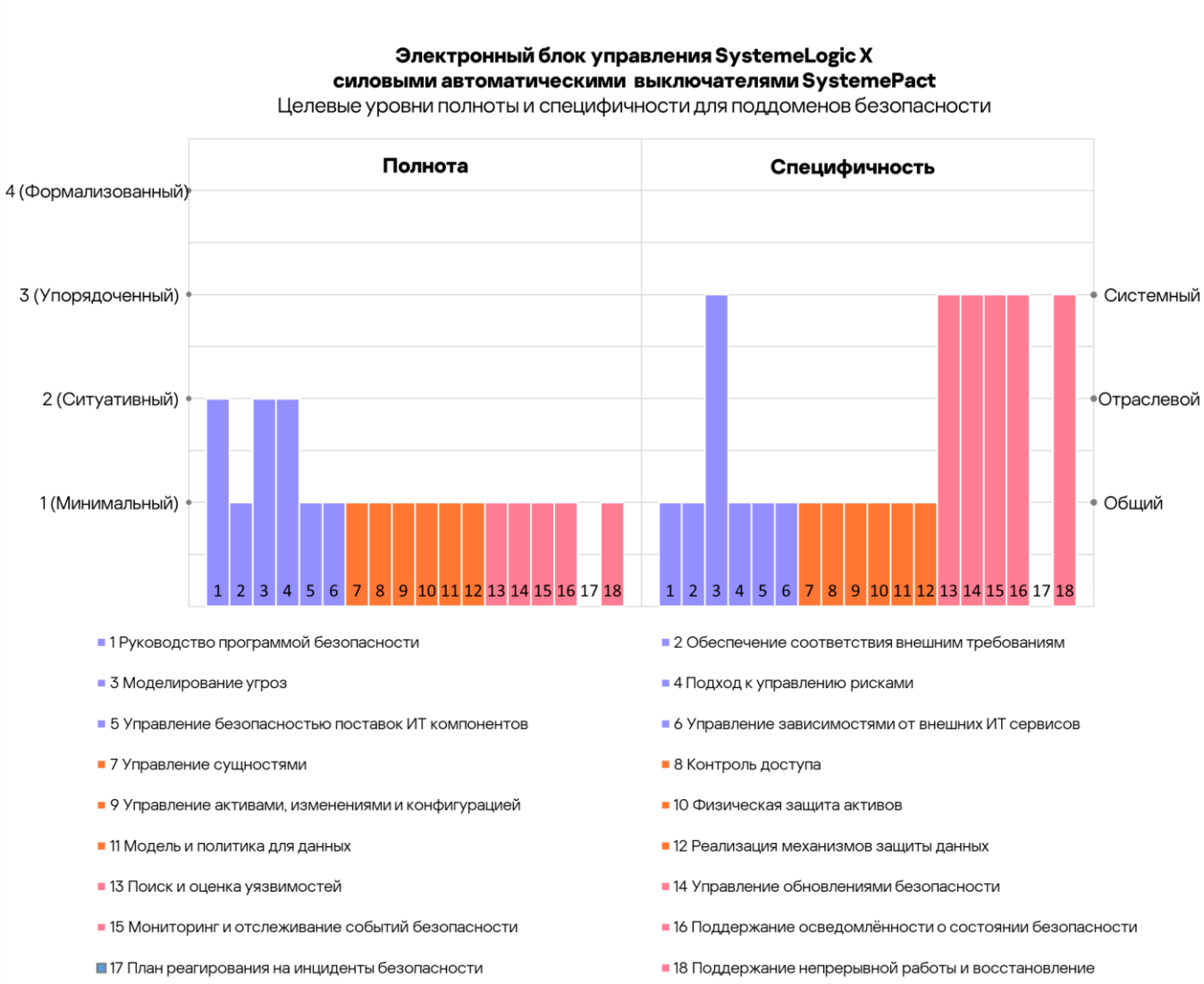
Поддомен	Потребности поддомена	Уровень полноты	Уровень специфичности
Стратегия и руководство	Определение наиболее подходящих методов обеспечения безопасности устройства	**1 / Минимальный**	**1 / Общий**
Угрозы и риски	Понимание системных и технологических уязвимостей	**2 / Ситуативный**	**1 / Общий**
Система поставок и внешние зависимости	Проверка репутации поставщиков и подрядчиков	**1 / Минимальный**	**1 / Общий**
Управление доступом	Поддержка элементарных сущностей для базового сценария использования	**1 / Минимальный**	**1 / Общий**
Защита активов	Учет использования как цифровых, так и физических активов	**1 / Минимальный**	**1 / Общий**
Защита данных	Обеспечение элементарных требований конфиденциальности и целостности данных	**1 / Минимальный**	**1 / Общий**
Уязвимости и обновления безопасности	Поддержание прошивки и компонентов устройства в актуальном состоянии и снижение подверженности атакам	**1 / Минимальный**	**3 / Системный**
Ситуационная осведомлённость	Минимальная осведомленность о событиях, связанных с безопасностью	**1 / Минимальный**	**3 / Системный**
Реагирование и восстановление	Проверка восстановления устройства после инцидентов	**1 / Минимальный**	**3 / Системный**

kaspersky

Целевые уровни полноты и специфичности реализации практик безопасности

Ниже приведены цели каждой практики обеспечения безопасности и соответствующие уровни полноты и специфичности целевого уровня зрелости безопасности для устройства.

Курсивом отмечены меры, необходимые для реализации соответствующей практики на конкретном уровне полноты и специфичности.



Практика безопасности	Назначение практики	Уровень полноты	Уровень специфичности
Руководство программой безопасности	Перечисление актуальных целей безопасности и способов их реализации *В компании должны быть разработаны и внедрены верхнеуровневая политика и отдельные процедуры по обеспечению кибербезопасности, которые распространяются на процессы разработки и управления уязвимостями.* *Задокументированный процесс безопасной разработки должен определять цели по созданию устройства, устойчивого для определенного спектра атак.*	**2 / Ситуативный**	**1 / Общий**
Обеспечение соответствия внешним требованиям	Обеспечение осведомлённости об основных факторах соответствия требованиям стандартов/регулятора *Ожидается, что устройство будет поставляться на различные промышленные и социальные объекты.* *Должен быть определен перечень стандартов и практик безопасности, релевантных для обеспечения безопасности процессов разработки и производства устройства. Должны быть идентифицированы те области, где требуется обеспечить соответствие данным стандартам и практикам.*	**1 / Минимальный**	**1 / Общий**
Моделирование угроз	Выявление и описание угроз на основе возможных сценариев функционирования *Угрозы должны ранжироваться исходя из обнаруженных в устройстве уязвимостей. Для оценки степени критичности уязвимостей должны применяться общепринятые и распространённые методы оценки, связанные с серьезностью уязвимостей.* *Специфичность:* *Моделирование угроз должно учитывать специфику применения устройства и соответствующие*	**2 / Ситуативный**	**3 / Системный**

Практика безопасности	Назначение практики	Уровень полноты	Уровень специфичности
	характерные последствия реализации угроз.		
Подход к управлению рисками	Дифференцирование важности рисков *Оценка рисков для устройства должна проводиться на основании оценки последствий отказа отдельных компонентов. Степень важности риска должна определяться на основе вклада связанного с ним компонента в отказ устройства.*	**2 / Ситуативный**	**1 / Общий**
Управление безопасностью поставок ИТ-компонентов	Отслеживание уязвимостей и патчей для поставляемых компонентов *Производитель должен реализовать процедуру выборочной проверки приобретаемых компонентов, в том числе аппаратных, в рамках требований системы менеджмента качества.* *Информация о доступных патчах и выявленных уязвимостях в ИТ-компонентах отслеживается в общедоступных источниках (официальный сайт поставщика, тематические ресурсы).*	**1 / Минимальный**	**1 / Общий**
Управление зависимостями от внешних ИТ-сервисов	Отслеживание репутации поставщиков внешних ИТ-сервисов *Архитектурой устройства не предусмотрено использование внешних инструментов и сервисов.* *Риски использования внешних сервисов в процессах разработки и производства должны минимизироваться в рамках договорных положений с поставщиками.*	**1 / Минимальный**	**1 / Общий**
Управление сущностями	Управление одной или несколькими сущностями схожим образом *Уникальный идентификатор устройства должен позволять однозначно идентифицировать конкретное устройство в среде установки и осуществлять его удалённую настройку.*	**1 / Минимальный**	**1 / Общий**

Практика безопасности	Назначение практики	Уровень полноты	Уровень специфичности
	Эксплуатационная документация должна содержать описание пользовательских ролей, которые могут использоваться для считывания данных и конфигурирования устройства.		
Контроль доступа	Ограничение возможности доступа внешних агентов к устройству *Доступ внешних подрядчиков и обслуживающих организаций должен регулироваться политиками и процедурами доступа на промышленном объекте.* *Доступ к устройству должен предоставляться для считывания информации, изменения настроек уставок или конфигурации.* *Устройство должно реализовывать простые механизмы ограничения доступа с целью изменения конфигурации устройства и настроек уставок с использованием пользовательских паролей.*	**1 / Минимальный**	**1 / Общий**
Управление активами, изменениями и конфигурациями	Отслеживание нечастых изменений в устройствах и их конфигурации *Пользовательская документация должна содержать рекомендации по установке и конфигурированию устройства.*	**1 / Минимальный**	**1 / Общий**
Физическая защита активов	Ограничение физического доступа к устройству или его компонентам в общих случаях *Конкретные меры физической защиты устройства должны определяться исходя из его сценария использования на промышленном объекте.* *Пользовательская документация должна содержать рекомендации по организации ограничения и контроля физического доступа к устройству.*	**1 / Минимальный**	**1 / Общий**
Модель и политика защиты данных	Заявление касательно защиты данных от несанкционированного доступа *Задокументированные процессы разработки и производства должны*	**1 / Минимальный**	**1 / Общий**

Практика безопасности	Назначение практики	Уровень полноты	Уровень специфичности
	определять некоторые требования к обеспечению защиты данных в устройстве, которые производитель считает достаточными. Требования к обеспечению безопасности паролей и данных, которые влияют на возможность доступа к устройству, должны устанавливаться, в том числе, исходя из соображений предотвращения неавторизованного доступа.		
Реализация механизмов защиты данных	Использование встроенных средств защиты для прошивки устройства *Прошивка должна обеспечивать сохранение целостности установленных параметров и событий мониторинга, а также их защиту от непреднамеренных изменений.* *Реализация механизмов защиты паролей и данных, которые влияют на возможность доступа к устройству, определяется требованиями к предотвращению неавторизованного доступа.*	**1 / Минимальный**	**1 / Общий**
Поиск и оценка уязвимостей	Рассмотрение широко известных уязвимостей *Должны рассматриваться и оцениваться известные уязвимости, которые потенциально могут присутствовать в используемых компонентах и технологиях.* *Специфичность:* *Оценка критичности уязвимостей должна проводиться в том числе исходя из их влияния на нормальную работу устройства.* *Оценка критичности (рейтинг CVSS) уязвимостей может переоцениваться, исходя из области применения устройства.* *Если уязвимость является унаследованной от переиспользуемого компонента, область действия уязвимости должна уточняться для каждого устройства, в котором используется компонент.*	**1 / Минимальный**	**3 / Системный**

Практика безопасности	Назначение практики	Уровень полноты	Уровень специфичности
Управление обновлениями безопасности	Учёт рекомендаций кибербезопасности от поставщиков отдельных компонентов устройства и установка соответствующих исправлений и патчей *Должна отслеживаться доступность новых версий программных компонентов.* *Обновления должны загружаться только из официальных источников и проходить тестирование согласно установленной методике испытаний перед внедрением в прошивку устройства.* *Специфичность:* *Управление обновлениями безопасности должно быть выстроено с учётом условий применения устройства, возможностью предварительного тестирования обновления в условиях применения, режимом доступа к устройству для проведения обновления, возможностью незамедлительного восстановления устройства при неудачном обновлении и требованиями к такому восстановлению в зависимости от условий применения. Соответствующие рекомендации должны быть включены в эксплуатационную документацию на устройство.*	**1 / Минимальный**	**3 / Системный**
Мониторинг и отслеживание событий безопасности	Периодическая проверка истории событий для диагностических целей *Должна проводиться проверка событий, связанных с изменением конфигурации или параметров устройства, на предмет идентификации их как относящихся к инцидентам безопасности.* *Специфичность:* *Возможности мониторинга ограничены вычислительными ресурсами устройства. Мониторинг применяется к типам событий, которые в том числе могут быть последствиями реализованной атаки на устройство, при оценке причин сбоя*	**1 / Минимальный**	**3 / Системный**

Практика безопасности	Назначение практики	Уровень полноты	Уровень специфичности
	устройства и расследовании инцидентов необходимо дифференцировать сбои, не связанные с нарушением кибербезопасности, и возможные компьютерные атаки, в том числе, с использованием данных мониторинга. *Соответствующие рекомендации должны быть включены в эксплуатационную документацию на устройство.*		
Поддержание осведомлённости о состоянии безопасности	Сбор релевантной информации из некоторых внешних источников *Должна поддерживаться осведомленность работников, занятых в разработке, производстве и сопровождении устройства: внутренние и внешние информационные рассылки в области ИБ, рассылки от вендоров, обмен информации с другими компаниями и исследователями компьютерной безопасности и т.д.* *Специфичность:* *Мероприятия по повышению осведомлённости работников должны включать сведения о технологиях и компонентах, применяемых в устройстве, необходимости сохранения авторизационных данных в тайне, недопустимости переиспользования авторизационных данных.* *Соответствующие рекомендации должны быть включены в эксплуатационную документацию на устройство.*	**1 / Минимальный**	**3 / Системный**
План реагирования на инциденты безопасности	***Для устройства практика не применима, поскольку оно является компонентом системы, для которой может разрабатываться соответствующий План реагирования.***	***Не применимо***	***Не применимо***
Поддержание непрерывной	Разработка основных инструкций по восстановлению устройства	**1 / Минимальный**	**3 / Системный**

Практика безопасности	Назначение практики	Уровень полноты	Уровень специфичности
работы и восстановление	*Пользовательская документация должна содержать рекомендации по восстановлению и настройке устройства после инцидентов кибербезопасности.* *Специфичность:* *Рекомендации по восстановлению должны учитывать специфику применения устройства, возможности незамедлительного восстановления при сбое, описание всех доступных способов восстановления работоспособности и безопасного состояния устройства.* *Соответствующие рекомендации должны быть включены в эксплуатационную документацию на устройство.*		

www.kaspersky.ru/

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