kaspersky

Программно-аппаратные платформы IP-камер видеонаблюдения Bosch

Целевой профиль зрелости безопасности
2021-0009-BOSCH-IPC

Kaspersky ICS CERT

27.09.2021

Содержание

Модель зрелости безопасности....3
Особенности подхода....3
Определение, назначение и структура модели....4
Целевой профиль зрелости безопасности....5
Объект оценки и область его использования....6
Факторы, учитываемые в ходе анализа....7
Целевые уровни полноты и специфичности реализации практик безопасности....9

Целевой профиль зрелости безопасности IP-камер видеонаблюдения Bosch

Задача этого документа – описать целевой профиль зрелости безопасности IP-камер видеонаблюдения Bosch, разработанный в соответствии с Моделью зрелости безопасности интернета вещей. Целевой профиль определяется производителем до проведения внешней оценки функций безопасности, их полноты и соответствия типу устройства, а также до любого дальнейшего улучшения этих функций

Модель зрелости безопасности

Не существует идеального решения, способного удовлетворить требования к безопасности для всех систем: каждая организация имеет собственные потребности, а разные системы требуют механизмы защиты разного уровня. Одна и та же технология в разных устройствах может применяться по-разному, в зависимости от конкретных требований.

Именно поэтому уровень защитных механизмов и процедур, отвечающих в полной мере требованиям безопасности конкретной организации, всегда будет разным. Организации могут сами устанавливать приоритеты выбора мер защиты, что позволяет использовать только те из них, которые решают поставленные задачи в области безопасности, и не задействовать ничего сверх необходимого.

Защитные механизмы и процессы считаются зрелыми,
если они позволяют достичь поставленных задач.

Особенности подхода

Уровень зрелости безопасности определяется не объективной строгостью механизмов безопасности, а возможностью достичь при их использовании требуемых целей. Следовательно, уровень зрелости безопасности – это мера достоверности того, что текущий уровень защиты отвечает всем требованиям безопасности организации. С другой стороны, уровень безопасности отражает тот факт, что система на текущий момент лишена уязвимостей и функционирует надлежащим образом.

У большинства организаций возникает необходимость определить,
на чем сосредоточить ограниченные ресурсы, выделенные на безопасность.

Это непростая задача, особенно в условиях постоянно меняющегося ландшафта угроз. Для определения текущего уровня безопасности и разработки стратегии безопасности на основе метрик необходимы количественные критерии и расстановка приоритетов. Цель модели зрелости безопасности – помочь производителям определить организационные и технические требования информационной безопасности и понять, как инвестировать в защитные механизмы, которые отвечают этим требованиям без лишних затрат на то, в чем нет необходимости.

Определение, назначение и структура модели

Модель зрелости безопасности, установленная *Консорциумом промышленного интернета вещей*, определяет уровни зрелости безопасности организации в зависимости от целей и задач организации, а также в зависимости от ее готовности принимать риски. Это позволяет ответственным лицам прилагать усилия к реализации только тех механизмов обеспечения безопасности, которые соответствуют конкретным требованиям организации.

Задача модели зрелости безопасности – определить требуемый[1] уровень зрелости безопасности организации и очередность действий, необходимых для его достижения.

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

Консорциум промышленного интернета вещей

Консорциум промышленного интернета вещей – мировой лидер в области решения проблем развития промышленного интернета вещей.

Наша задача – донести компаниям, отраслям промышленности и обществу преобразующую коммерческую ценность, ускоряя внедрение надежного интернета вещей.

Консорциум промышленного интернета вещей является проектом компании Object Management Group®, Inc. (OMG®).

Дополнительные сведения приведены на веб-сайте www.iiconsortium.org.

Иерархия практик зрелости безопасности

Ядро модели зрелости безопасности представлено иерархией практик обеспечения безопасности. На рисунке 1 показана модель зрелости безопасности с разбивкой по доменам.

Домены – это верхний уровень, охватывающий ключевые аспекты зрелости безопасности: управление требованиями; реализация мер защиты; усиление мер защиты.

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 каждом поддомене для достижения определенных результатов может использоваться ряд практик 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.

[1] Англ. required

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.

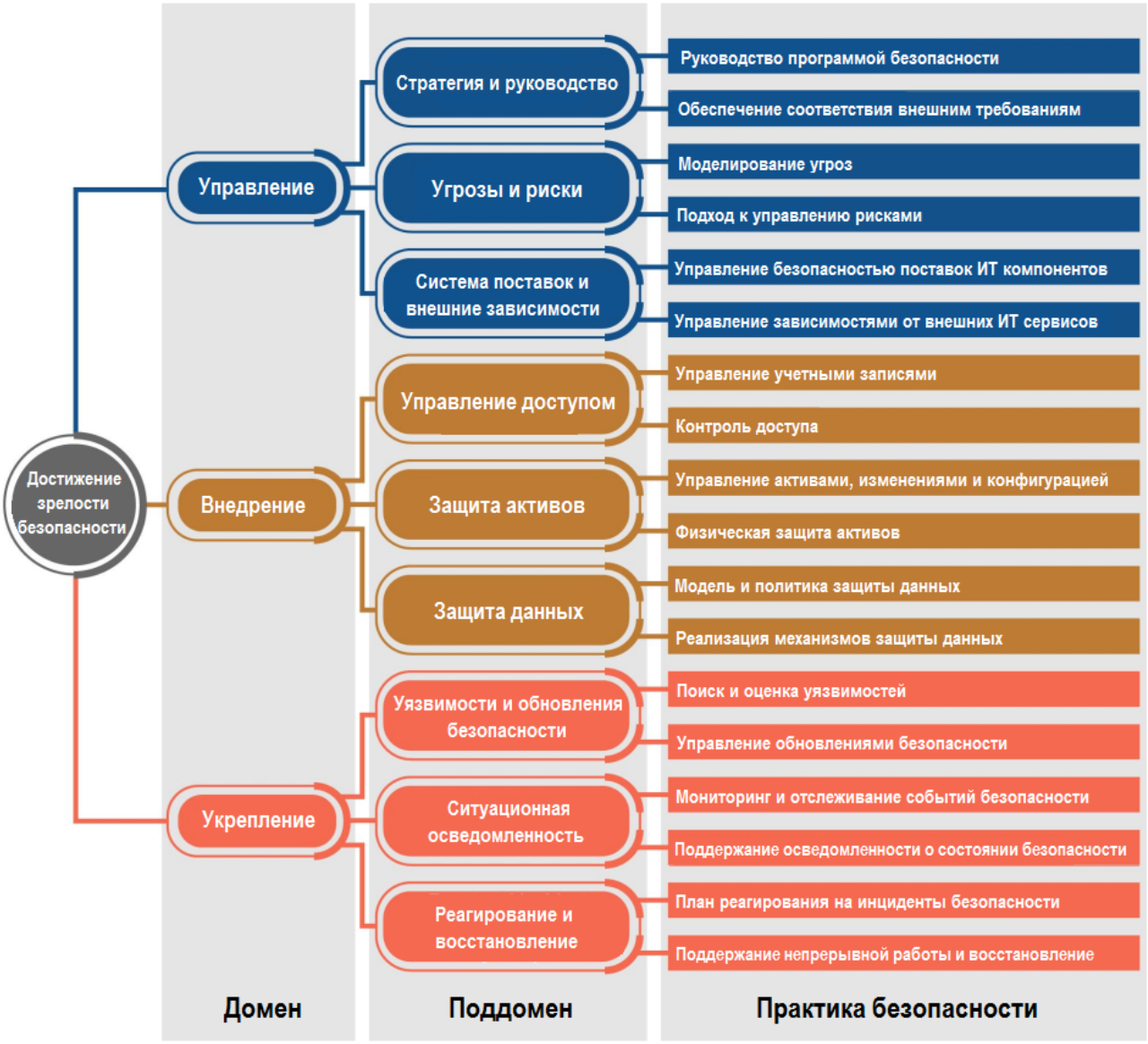

Рис. 1. Иерархия модели зрелости безопасности интернета вещей

Целевой профиль зрелости безопасности

В этом разделе приведены результаты анализа в соответствии со специфичными для устройств факторами, описанными ниже. Анализ целевого уровня зрелости безопасности проводился для каждого из

трех уровней: домены, поддомены и практики. Процесс определения уровней зрелости описан в следующем разделе.

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 объема (степени соответствия отраслевым и системным задачам) требований к безопасности с инвестициями в соответствующие практики.

Целевой профиль зрелости безопасности описывает
максимальный уровень зрелости безопасности данной системы.

Он включает последовательный набор практик обеспечения безопасности, предоставляющий всем ответственным лицам понимание и общих целей, и целей каждой конкретной практики.

Объект оценки и область его использования

Целью этого проекта является оценка и повышение безопасности программно-аппаратных платформ IP-камер видеонаблюдения Bosch.

IP-видео (видео, передаваемое по протоколу IP) распространяется все шире в современной сетевой среде. При размещении любого IP-устройства в сети защита сети от атак также зависит от функций и возможностей обеспечения безопасности самого устройства. Не существует универсального решения для обеспечения безопасности всех устройств видеонаблюдения. В разных ситуациях требуются разные меры обеспечения безопасности видео.

В то же время производитель хочет подтвердить, что существующие возможности обеспечения безопасности каждого устройства являются достаточными для того, чтобы в долгосрочной перспективе гарантировать отсутствие серьезных причин для беспокойства в отношении безопасности данных и видео.

Объектом данной оценки являются следующие IP-камеры видеонаблюдения:

- FLEXIDOME IP starlight 8000i - 8MP (*NDE-8504-R*)
- FLEXIDOME IP micro 3000i (*NDV-3502-F03*)

Для анализа уязвимостей, проводимого в рамках оценки уровня зрелости безопасности, были предоставлены следующие IP-камеры:

- FLEXIDOME IP starlight 8000i - 8MP (*NDE-8504-R*)
- FLEXIDOME IP micro 3000i (*NDV-3502-F03*)

Сходство функционального назначения, встроенного программного обеспечения и процессов, реализованных для обеспечения функций безопасности, позволяет распространить результаты этой оценки на следующие камеры:

CPP14

1. FLEXIDOME multi 7000i
2. FLEXIDOME panoramic 5100i

CPP13

1. AUTODOME inteox 7000i
2. MIC inteox 7100i

CPP7.3

1. AUTODOME IP 4000i
2. AUTODOME IP 5000i
3. AUTODOME IP starlight 5000i (IR)
4. AUTODOME IP starlight 7000i
5. DINION IP 3000i
6. DINION IP bullet 4000i
7. DINION IP bullet 5000
8. DINION IP bullet 5000i
9. DINION IP bullet 6000i
10. FLEXIDOME IP 3000i
11. FLEXIDOME IP 4000i
12. FLEXIDOME IP 5000i
13. FLEXIDOME IP starlight 5000i (IR)
14. FLEXIDOME IP starlight 8000i
15. MIC IP starlight 7000i
16. MIC IP starlight 7100i
17. MIC IP ultra 7100i
18. MIC IP fusion 9000i

CPP7

1. DINION IP starlight 6000
2. DINION IP starlight 7000
3. DINION IP thermal 8000
4. FLEXIDOME IP starlight 6000
5. FLEXIDOME IP starlight 7000
6. DINION IP thermal 9000 RM

CPP6

1. AVIOTEC IP starlight 8000
2. DINION IP starlight 8000 12MP
3. DINION IP ultra 8000 12MP

Факторы, учитываемые в ходе анализа

Область применения. Компания Bosch имеет надежную репутацию одного из ведущих поставщиков комплексных решений для видеонаблюдения, как базовых, так и многокомпонентных. Широкий ассортимент продуктов Bosch включает проводные и беспроводные IP-камеры, PTZ-камеры, камеры AutoDome, видеокодеры, цифровые видеорегистраторы, сетевые видеорегистраторы и многое другое. Одна из специализаций компании – предоставление пользователям инструментов, необходимых для интеграции существующих камер в новые, более продвинутые сетевые системы наблюдения. Передовые кодеры и продукты Bosch являются средствами для создания сложных, гибких и легко масштабируемых систем видеонаблюдения. Все эти факторы значительно расширяют сферу применения IP-камер Bosch.

Подверженность атакам. Пути взлома IP-камер легко определить: через интернет, инфраструктуру видеонаблюдения (другие подключенные устройства, рекордеры, средства просмотра, серверы управления) или посредством физического доступа.

Ландшафт угроз. IP-видеоустройства являются типичной целью удаленных атак, как стихийных, так и направленных на конкретный тип устройства или инфраструктуру, поддерживающую наблюдение за определенной областью или объектом. Например, ботнет Mirai, появившийся в 2016 году и нацеленный на цифровые видеорегистраторы, камеры видеонаблюдения и другие устройства, все еще представляет угрозу безопасности интернета вещей. Такие ботнеты используются для проведения крупномасштабных

атак, направленных одновременно на несколько целей. С момента публикации исходного кода ботнета Mirai вредоносные программы постоянно совершенствуются и дополняются новыми функциями и эксплойтами.

Актуальность. IP-видеокамера не является принципиально новым устройством, и обеспечение безопасности, без сомнения, является одной из ее основных задач. Для IP-камер существуют практические рекомендации, а также нормативные и стандартные требования обеспечения безопасности. Также существуют конкретные рекомендации поставщиков по усилению защиты IP-видеоустройств Bosch.

Релевантность. Иногда инциденты безопасности, связанные с IP-камерами, обсуждаются открыто. Однако такие инциденты происходят постоянно, даже если не афишируются. Bosch регулярно выпускает рекомендации по безопасности, чтобы информировать клиентов об обнаруженных уязвимостях в своих продуктах и сервисах.

Безотлагательность. В системе безопасности IP-камер существуют известные уязвимости. Также существует ненулевая вероятность обнаружения новых уязвимостей в ближайшее время. С точки зрения безопасности особого внимания требуют технологии и сервисы, предназначенные для внешнего доступа и управления устройствами.

Ущерб от угроз. Успешно проведенная атака может вызвать сбой в работе IP-камеры и даже повлиять на безопасность всей инфраструктуры. В случае видеонаблюдения особенно актуальны вопросы конфиденциальности, например недопущение несанкционированного раскрытия видео с участием определенных лиц, которые могут оказаться узнанными.

Сложности и ограничения. Основной сложностью является необходимость поддержки прямой непрерывной трансляции и записи видео в большинстве мест, где используется видеонаблюдение. Любой простой приводит к серьезным сбоям. Таким образом, первостепенное значение имеет упрощенная конфигурация, сокращенное время обучения и простота эксплуатации всех функций устройства, включая функции безопасности.

Предпосылки доверия. Вся инфраструктура видеонаблюдения должна быть защищена надлежащим образом. Некоторые аспекты безопасности зависят от конфигурации сервера видеонаблюдения. В некоторых случаях может быть нарушена конфиденциальность при хранении видеозаписей. IP-камеры производятся с учетом того, что остальная инфраструктура и отдельные ее компоненты защищены должным образом. Все модели IP-камер Bosch, участвующие в оценке, имеют надежные криптопроцессоры, выполняющие функции аппаратной защиты. Различные компоненты инфраструктуры имеют разные уровни защиты, и чтобы предотвратить непреднамеренное нарушение безопасности инфраструктуры необходимо четко определить доверенные компоненты.

Распределение работ по времени. Bosch расценивает безопасность камеры как неотъемлемый атрибут качественного продукта, поэтому для обеспечения соответствия стандартам безопасности для всех проектов камер должен выполняться анализ угроз и рисков. Bosch выделяет время и ресурсы на разработку и реализацию систем и функций безопасности, однако из-за возросшей конкуренции на рынке итоговая стоимость и ограничения времени разработки влияют на остаточный уровень риска системы безопасности устройства.

Ожидаемые результаты от выполнения работ. Важно сосредоточиться на усилении защиты IP-камер, принимая во внимание известные инциденты безопасности и распространенные технологические уязвимости. Приоритетными являются методы моделирования угроз и усиления защиты. Зрелость организации операционных работ должна соответствовать ожидаемому уровню защиты инфраструктуры.

Зависимости работ. Управление безопасностью поддерживает меры по усилению мер защиты, что должно быть учтено при планировании улучшения соответствующих практик безопасности.

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 IP-видеокамер Bosch.

Практика безопасности	Назначение практики	Уровень полноты	Уровень специфичности
Руководство программой безопасности	Охватить основные требования признанных стандартов управления безопасностью. Это означает создание программы безопасности, согласованной с организационной структурой компании и ее системами.	**3 / Упорядоченный**	**Общий**
Обеспечение соответствия внешним требованиям	Рассмотреть возможность выполнения некоторых дополнительных требований, касающихся соответствия стандартам, регуляторным актам и специальным нормативным документам. Это означает проведение анализа и интерпретации требований, касающихся соответствия стандартам, регуляторным актам и специальным нормативным документам.	**2 / Ситуативный**	**Общий**
Моделирование угроз	Точно описать и классифицировать угрозы (необязательно формальным образом). Это означает, что анализ уязвимостей для выявления и устранения угроз выполняется по ситуации в соответствии с результатами анализа рисков.	**2 / Ситуативный**	**Общий**
Подход к управлению рисками	Оценить уровень рисков и должным образом управлять ими. Это означает, что разрабатываются процедуры детализированной оценки рисков и проводится классификация рисков по степени важности.	**3 / Упорядоченный**	**Общий**

Управление безопасностью поставок ИТ-компонентов	Провести тестирование безопасности поставляемых компонентов. Это означает выполнение анализа влияния цепочки поставок на безопасность, обеспечение базовой защиты на уровне соглашений и применение методов для отслеживания угроз со стороны цепочки поставок.	**2 / Ситуативный**	**Общий**
Управление зависимостями от внешних ИТ-сервисов	Обеспечить качество сервисов. Это достигается посредством заключения соглашений об уровне обслуживания с указанием в этих соглашениях метрик обеспечения качества и безопасности. Bosch устанавливает конкретные требования в влиянию сервисов на работу устройства. В частности, доступность устройства должна поддерживаться даже в случае сбоя внешних сервисов. Это специальное требование, обусловленное необходимостью непрерывности работы камеры, поэтому уровень специфичности этой практики меняется на «системный».	**2 / Ситуативный**	**Системный**
Управление учетными записями	Управлять учетными записями групп людей, систем или вещей.	**1 / Минимальный**	**Общий**
Модель и политика защиты данных	Разработать простую категоризацию данных и соответствующие ограничения на использование и модификацию данных. Разработка систем классификации данных, например для выявления типов данных, содержащих информацию, охраняемую законом. Поскольку вся ответственность за защиту данных лежит на клиенте, Bosch не может предложить более конкретные меры для поддержки конкретных политик. Однако при ситуативном подходе уровень детализации, доступный на стороне Bosch, учитывается должным образом для	**2 / Ситуативный**	**Общий**

	определения политики защиты данных.		
Реализация механизмов защиты данных	Обеспечить безопасность данных при помощи технических, программных (и, если требуется, организационных) средств в соответствии с релевантными требованиями стандартов в области защиты информации. Эта практика включает внедрение последовательных и непрерывных мер защиты данных по всей системе.	**3 / Упорядоченный**	**Общий**
Поиск и оценка уязвимостей	Получить объективную стороннюю оценку уязвимостей. Это означает выполнение комплексного анализа уязвимостей IP-камеры в целом с использованием автоматизации и с учетом сторонних оценок.	**3 / Упорядоченный**	**Общий**
Управление обновлениями безопасности	Обеспечить соблюдение системной политики, гарантирующей непрерывную защиту от известных атак. Это означает обеспечение защиты компонентов с длительным жизненным циклом, уязвимости которых нелегко закрыть исправлениями безопасности из-за сертификационных или эксплуатационных требований. Bosch ограничивает внедрение этой практики (автоматическое применение обновлений) из-за возможных операционных ограничений на стороне клиента. Например, видеонаблюдение нельзя остановить в произвольный момент для установки обновлений. Это специальное требование, обусловленное необходимостью непрерывности работы камеры, поэтому уровень специфичности этой практики меняется на «системный».	**4 / Формализованный**	**Системный**
Мониторинг и отслеживание	Периодически проверять события, чтобы оценить, правильно ли	**2 / Ситуативный**	**Системный**

событий безопасности	выполняются критические процессы. Это предполагает получение информации о состоянии устройств видеонаблюдения и проверку правильности работы системы. При реализации этой практики имеются некоторые ограничения. Обнаружение вредоносного ПО расценивается специалистами Bosch как излишняя практика (для проприетарной операционной системы специальное вредоносное ПО до сих пор не было обнаружено, хотя это не значит, что оно не может существовать). При реализации мониторинга необходимо поддерживать максимальную продолжительность работы устройства, не подвергая его диагностическим действиям. Это специальное требование, обусловленное необходимостью непрерывности работы камеры, поэтому уровень специфичности этой практики меняется на «системный».		
Поддержание осведомленности о состоянии безопасности	Разработать и реализовать процедуры предоставления внутренних данных официальным органам и общественности по каждому конкретному факту компрометации устройств или данных. Это обеспечивает поддержку общей осведомленности о внешних инцидентах и реализацию политики раскрытия информации об инцидентах внешним сторонам на основе принципа служебной необходимости.	**3 / Упорядоченный**	**Общий**
План реагирования на инциденты безопасности	Описать конкретные инциденты и основные ответные действия. Сюда входит предоставление рекомендаций по обнаружению и реагированию на инциденты, которые могут повлиять на критические компоненты системы. Для этой практики рассматривается только минимальный уровень, поскольку	**1 / Минимальный**	**Системный**

	ответственность за обнаружение событий и реагирование на них лежит на клиенте. Не всегда есть возможность реагировать на инцидент незамедлительно, поскольку камера может в этот момент использоваться. Это специальное требование, обусловленное необходимостью непрерывности работы камеры, поэтому уровень специфичности этой практики меняется на «системный». Также уменьшается количество применимых методов реагирования на события.		
Поддержание непрерывной работы и восстановление	Предоставлять основные инструкции по восстановлению системы. Исправление и восстановление можно выполнить только при доступности камеры в зависимости от режима наблюдения и размещения камеры. Это специальное требование, обусловленное необходимостью непрерывности работы камеры и ее возможным расположением в физически малодоступном месте, поэтому уровень специфичности этой практики меняется на «системный».	**1 / Минималистичный**	**Системный**

Рис. 2. Определение целевого профиля зрелости безопасности

kaspersky

www.kaspersky.ru/

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