kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Антон Шипулин

Менеджер по развитию решений по промышленной кибербезопасности, АО «Лаборатория Касперского»

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

kaspersky

Инвентаризация активов АСУ ТП: Вы не можете защитить то, что вы не знаете

Anton Shipulin

Kaspersky Industrial Cybersecurity Conference 2020

Обо мне

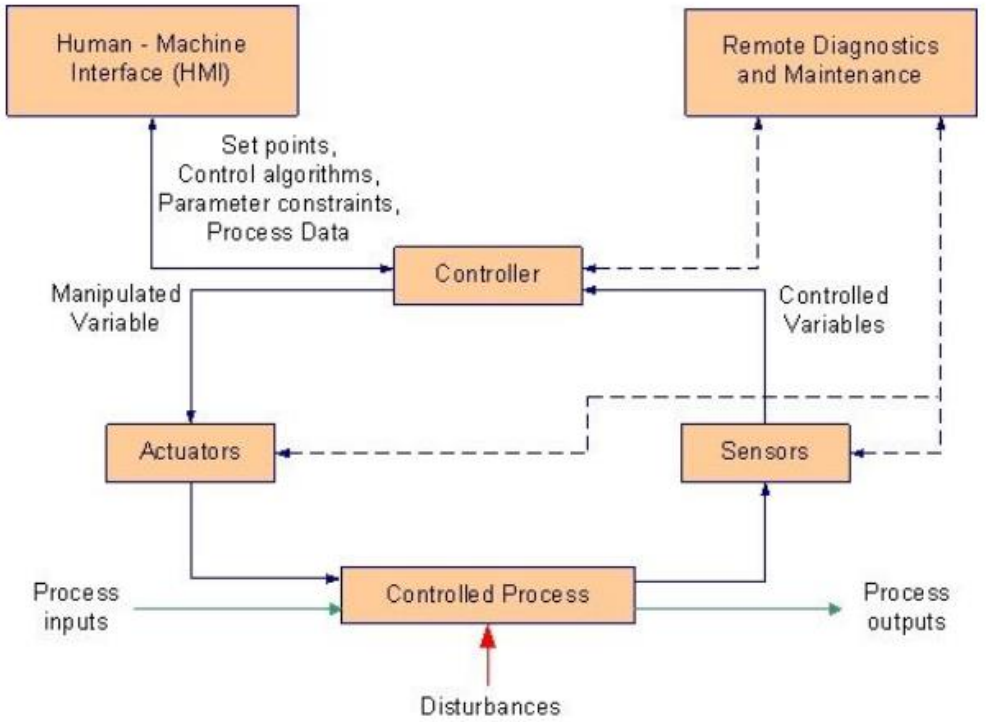
kaspersky RUSCADASEC Industrial Cybersecurity Center

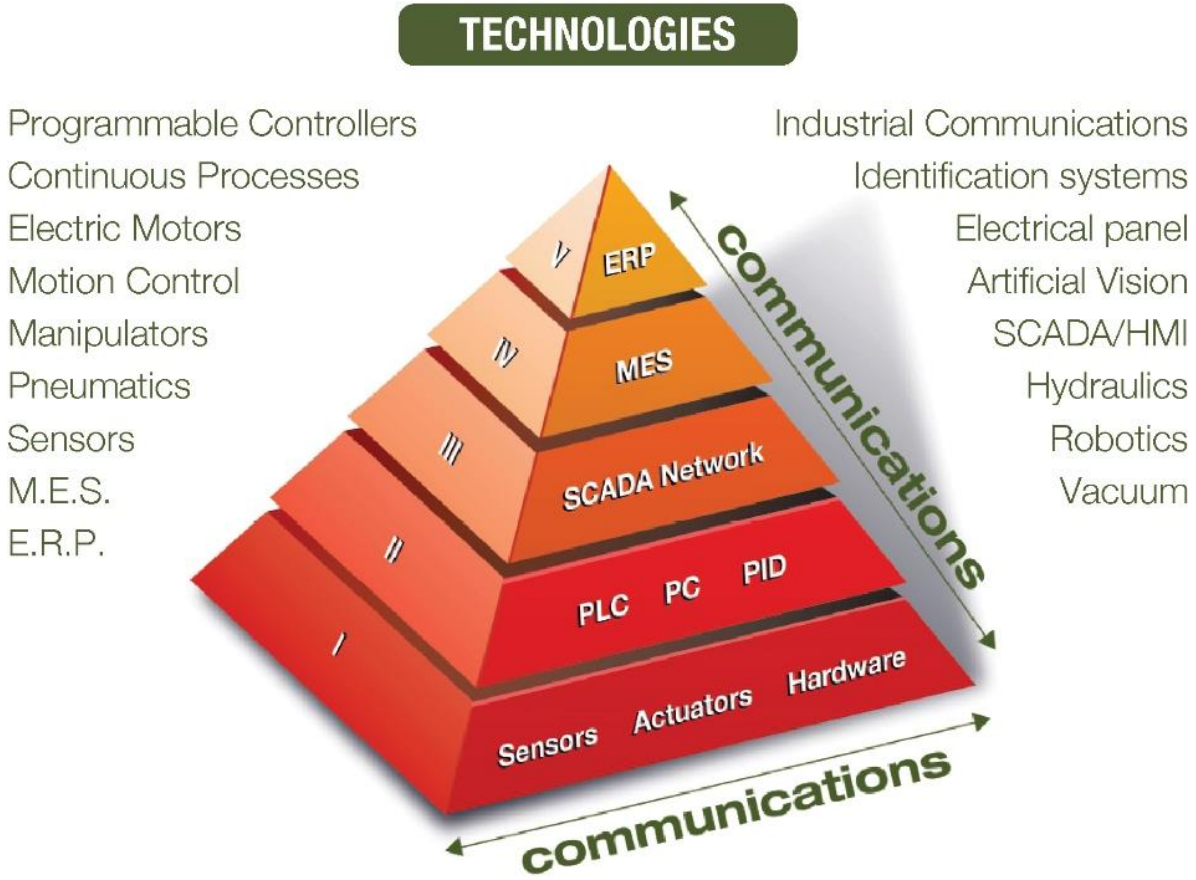
- Развитие бизнеса Industrial Cybersecurity @ **Kaspersky**
- Руководитель программного комитета **KICS con**
- Координатор в России @ **Industrial Cybersecurity Center** (**CCI**)
- Сооснователь сообщества **RUSCADASEC:** t.me/RUSCADASEC
- Certified SCADA Security Architect (**CSSA**), **CISSP**, **CEH**

План

- Проблема инвентаризации активов
- Рекомендации и стандарты
- Подходы к инвентаризации активов
- Процесс построения инвентаризации
- Выгоды для бизнеса
- Выводы

Усложнение промышленной среды





https://www.smctraining.com/en/webpage/indexpage/312

Вызов: вы не можете защитить то, что вы не знаете

В последние годы мы видим, АСУ ТП уязвимы для кибер инцидентов. Осведомленность растет, и все больше и больше организаций внедряют меры безопасности для повышения уровня кибербезопасности своих устройств и сетей. Однако остается повторяющаяся проблема: **недостаточная осведомленность об объеме и общем количестве активов, которыми владеет организация.**

Незнание границ затрудняет принятие мер по защите устройств, поэтому некоторые из них останутся незащищенными. Исходя из принципа, **что сила цепи определяется ее самым слабым звеном**, мы можем сделать вывод, что, если мы не обеспечим одинаковую защиту всех активов, этих мер будет недостаточно.

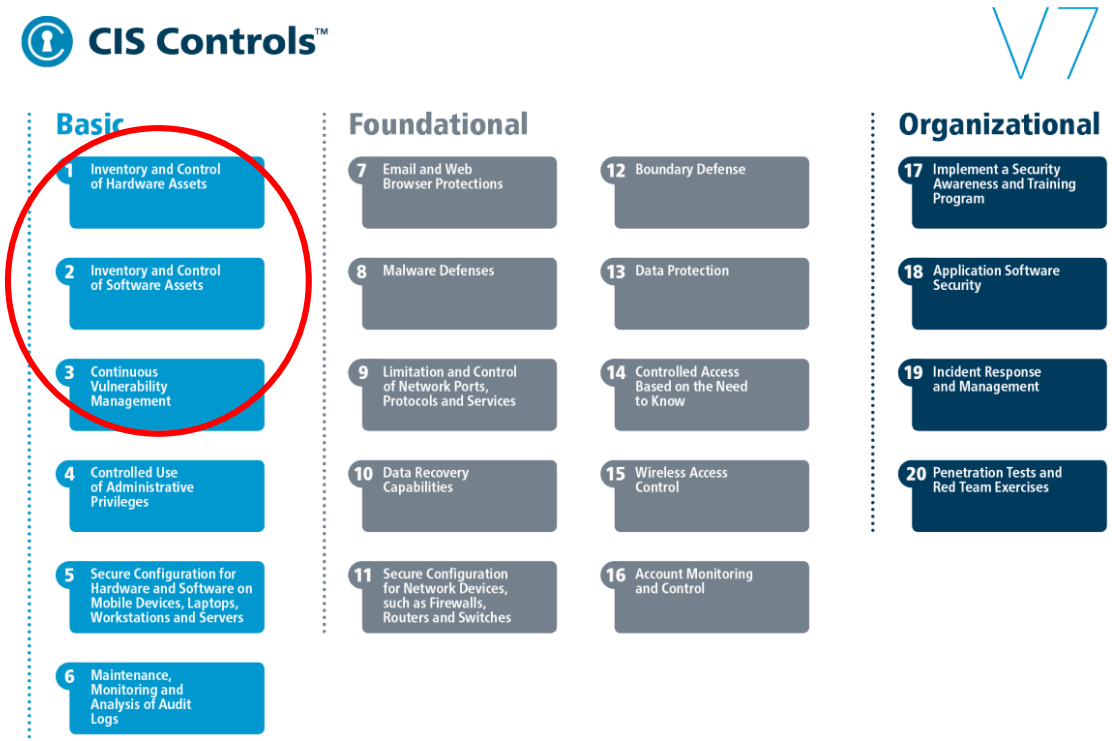
Поэтому **первым шагом** в обеспечении безопасности **АСУ ТП** является инвентаризация всех активов, задействованных в процессе. Эта инвентаризация, если все сделано правильно, будет собирать подробную информацию по каждому активу, включая версии программного обеспечения или микропрограмм. Имея эту информацию, инвентаризация может использоваться для правильного управления уязвимостями, что позволит принять необходимые меры для их устранения и смягчения.

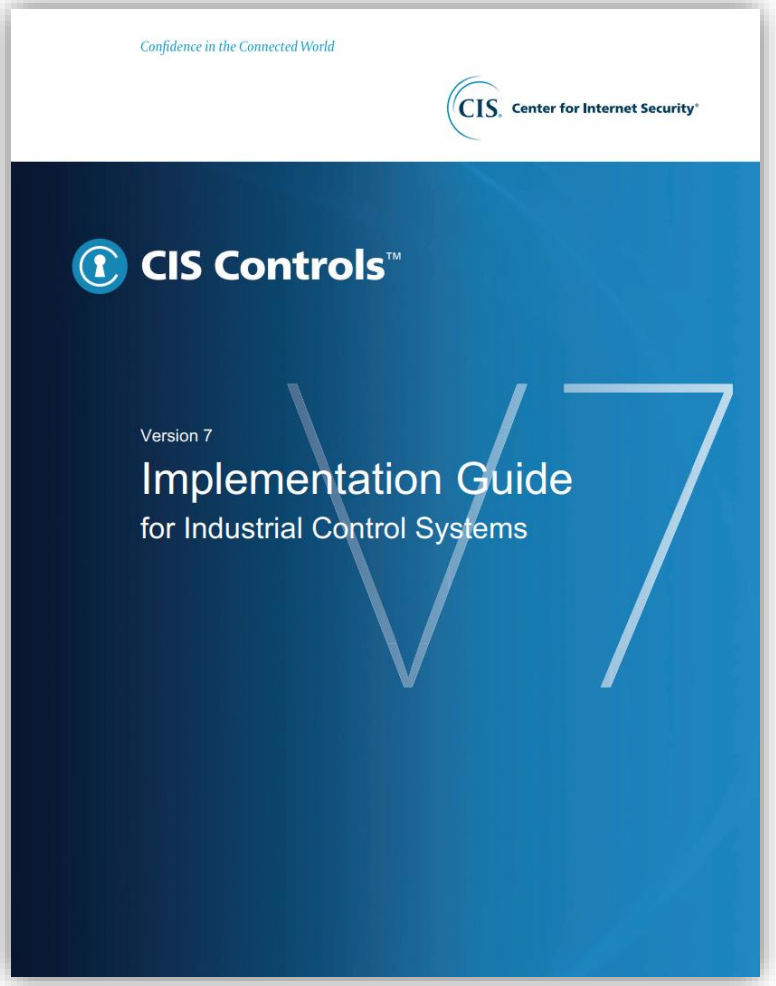
Кибербезопасность систем промышленной автоматизации в 2019 году
https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

INCIBE-CERT. Guide for an asset inventory management in industrial control systems
https://www.incibe-cert.es/en/publications/guides/guide-asset-inventory-management-industrial-control-systems

Инвентаризация активов в стандартах: CIS 20

The CIS Controls™ - приоритезированный набор мер, которые в совокупности образуют набор передовых практик для эшелонированной защиты, которые смягчают наиболее распространенные атаки на системы и сети.





https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/

Инвентаризация активов в стандартах

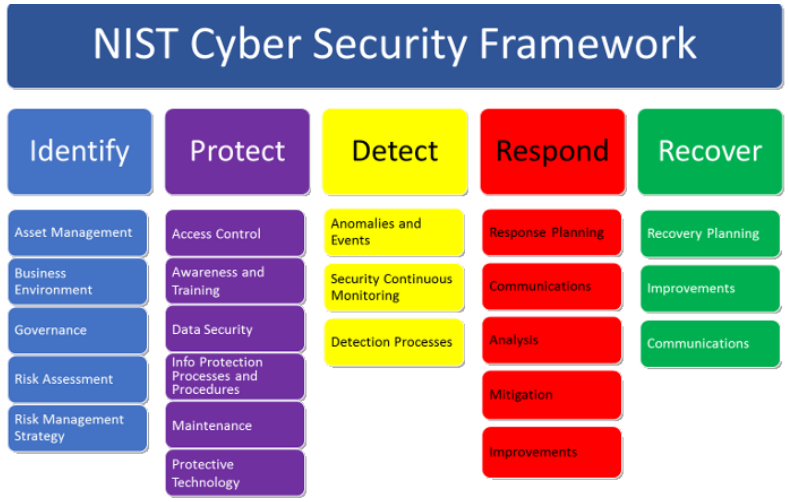
AuditScripts	Critical Security Controls	enclave SECURITY						
Critical Security Control	**NIST CSF v1.1**	**NIST 800-82 rev2**	**IEC 62443-3-3:2013**	**NERC CIP v7**	**NERC CIP v6**	**NERC CIP v5**	**NERC CIP v4**	**NERC CIP v3**
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	ID.AM-1 ID.AM-3 ID.AM-4 PR.DS-3	6.2.16 6.2.17	SR 1.2 SR 2.3 SR 7.8	CIP-002-5.1 R1 CIP-002-5.1 R2	CIP-002-5.1 R1 CIP-002-5.1 R2	CIP-002-5.1 R1 CIP-002-5.1 R2	CIP-002-4 R1 CIP-002-4 R2 CIP-002-4 R3 CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-006-4 R3	CIP-002-3 R1 CIP-002-3 R2 CIP-002-3 R3 CIP-002-3 R4 CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-006-3 R3
Critical Security Control #2: Inventory of Authorized and Unauthorized Software	ID.AM-2 PR.DS-6	6.2.16 6.2.17	SR 1.2	CIP-010-3 R1	CIP-010-2 R1	CIP-010-1 R1		
Critical Security Control #3: Continuous Vulnerability Assessment and Remediation	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.AN-5 RS.MI-3	6.2.16 6.2.17		CIP-007-6 R2 CIP-010-3 R3	CIP-007-6 R2 CIP-010-2 R3	CIP-007-5 R2 CIP-010-1 R3	CIP-005-4 R4 CIP-007-4 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8
Critical Security Control #4: Controlled Use of Administrative Privileges	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3	5.15 6.2.7 6.2.16 6.2.17		CIP-004-6 R4 CIP-004-6 R5 CIP-007-6 R5	CIP-004-6 R4 CIP-004-6 R5 CIP-007-6 R5	CIP-004-5 R4 CIP-004-5 R5 CIP-007-5 R5	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-005-4 R3 CIP-006-4 R3 CIP-007-4 R3	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-005-3 R3 CIP-006-3 R3 CIP-007-3 R3

https://www.auditscripts.com/wp-content/uploads/dlm_uploads/2016/04/AuditScripts-Critical-Security-Control-Master-Mappings-v7.0d.xlsx

Инвентаризация активов в стандартах

The NIST Cybersecurity Framework - Рекомендации по кибербезопасности, для организаций частного сектора и критической инфраструктуры оценки и совершенствования своих процессов по предотвращению, обнаружению и реагированию на кибер риски.

https://www.nist.gov/cyberframework

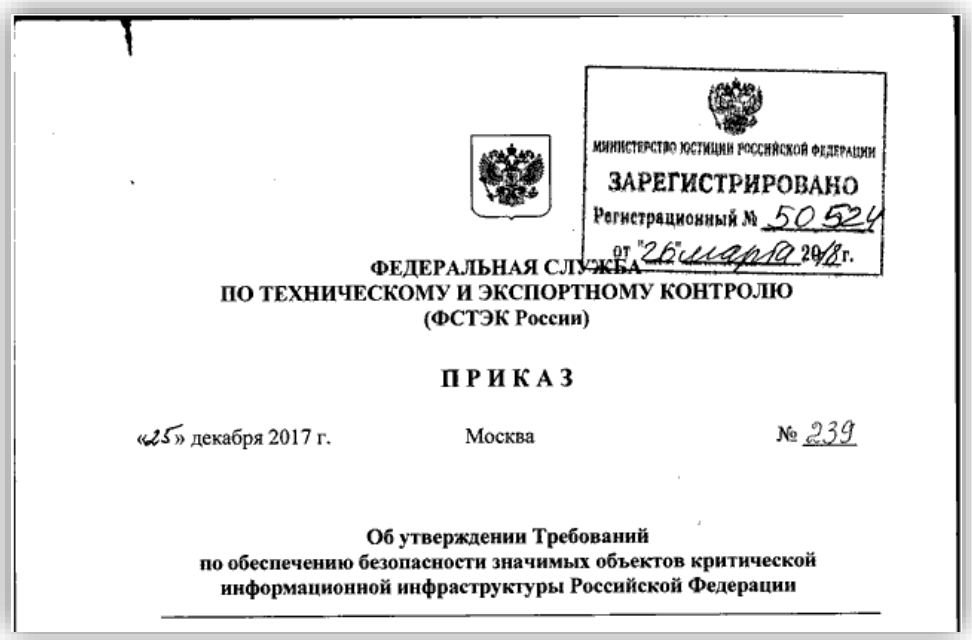


Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Управление активами в России

Приказ ФСТЭК России №239 «Об утверждении Требований по обеспечению безопасности ЗО КИИ РФ»

- I. Идентификация и аутентификация (ИАФ)
- V. Аудит безопасности (АУД)
- XIII. Управление конфигурацией (УКФ)
- XIV. Управление обновлениями ПО(ОПО)



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от "26" марта 2018 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«25» декабря 2017 г. Москва № 239

Об утверждении Требований
по обеспечению безопасности значимых объектов критической
информационной инфраструктуры Российской Федерации

Приказ ФСТЭК России №239 «Об утверждении Требований по обеспечению безопасности ЗО КИИ РФ»
https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

Подходы к инвентаризации активов

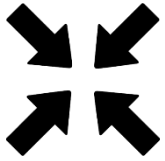
Physical Inspection & Manual

Ручная инвентаризации без автоматизации, обычно с использованием таблиц Excel. Требует много времени и трудозатрат, подвержено человеческим ошибкам и неполным данным, его сложно поддерживать и обновлять. Может быть эффективным только для первоначальной инвентаризации, для небольшого количества устройств и для некоторых чувствительных объектов.

Configuration files analysis

Автоматизированный подход и берет существующие данные конфигурации (включая теги) из систем управления процессами, сетевых устройств, диаграмм процессов и других источников конфигурации для создания профиля активов. Отличный способ получить информацию об АСУ ТП, которую нельзя получить другими методами, например для изолированных и отключенных сред, таких как системы ПАЗ

Passive Inventory / Listening



Автоматизированный подход, который «слушает» и анализирует копию сетевого трафика АСУ ТП через SPAN порты или TAP устройства для получения информации об активах. Он на 100% безопасен для сетей АСУ ТП, не влияет на активы, но, поскольку он прослушивает только «взаимодействующие устройства», он получает меньше информации от каждого актива.

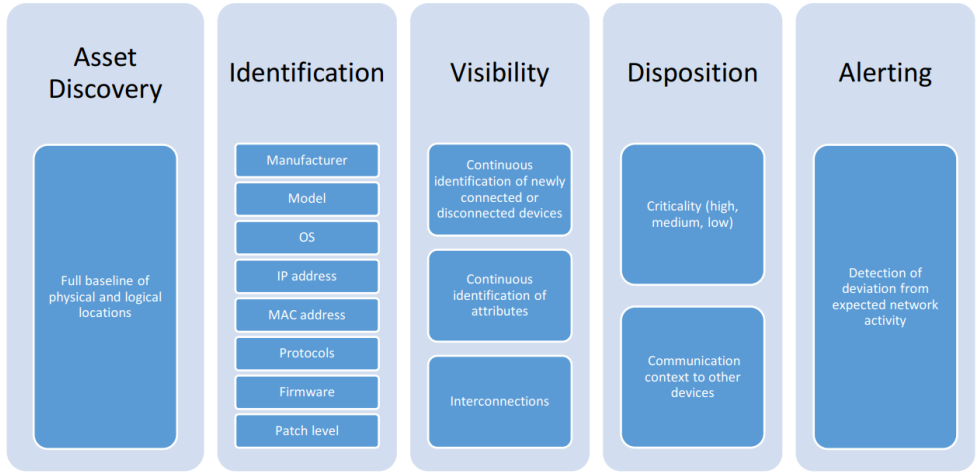
Active Inventory / Probing

Автоматизированный метод, который активно опрашивает устройства АСУ ТП об информацию об активах на «родном» языке промышленного протокола. Быстро обнаруживает сетевые коммуникации и детали активов. Может вызвать повреждение объекта при взаимодействии с ним, поэтому следует использовать с осторожностью.

Атрибуты активов

Чтобы инвентаризация была полезна с точки зрения безопасности и управления рисками, важно хранить подробную информацию о каждом активе, включенном в него. Некоторые из наиболее важных атрибутов, которые должны быть собраны для каждого актива:

Figure 3-2 Asset Management Characteristics

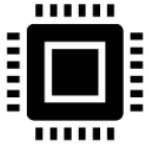


NCCoE, NIST Cybersecurity Practice Guide, SP 1800-23, Energy Sector Asset Management.
https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management

- Unique asset ID
- Asset type / function
- Asset state information (Running, stop, etc.)
- Asset name
- Description
- Network name
- Domain / workgroup
- Manufacturer
- Model number
- Serial number
- Sub-assets (such as daughter cards)
- Impact on operations
- Asset Criticality
- Physical location
- Logical location / Business unit
- Purdue Level
- Firmware / OS revision
- Software versions
- Software vulnerabilities (CVE)
- Cybersecurity risk score
- Patch levels
- Hardware components (CPU, modules, etc.)
- IP addresses
- MAC addresses
- Communication role (client/server, master/slave)
- Network media (Ethernet, serial, fiber)
- Connected wire tags/circuit information
- Network Protocols in use (ICS and IT)
- Open network ports
- Location of configuration information
- Location of configuration offline backup
- Associated I/O points or tags
- Asset owner and contact Info
- Asset Manager
- Process owner and contact Info
- Links to parent assets
- Links to child assets
- Licensing details
- Asset Cost
- Maintenance dates
- End-of-life dates

Классификация активов

Активы АСУ ТП важные для безопасности – это не только сетевые устройства. Нужно понимать весь контекст систем, и стремиться контролировать как можно больше активов и их параметров, и взаимодействие между ними

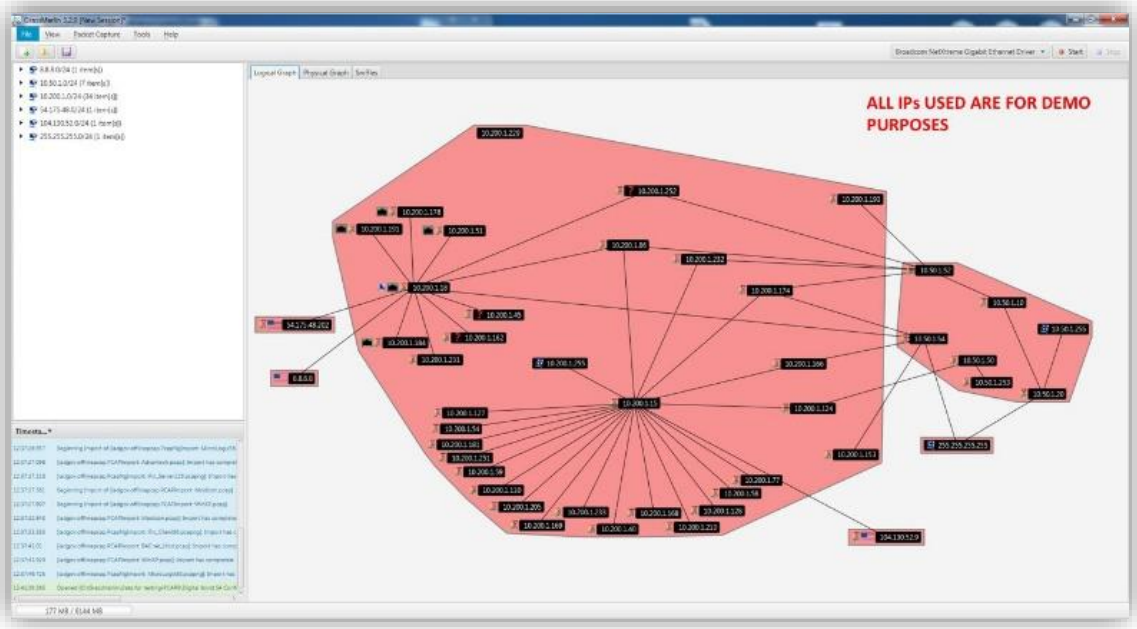
Asset		Description	Examples
Hardware		All physical equipment used in the development of the industrial process.	■ PLC ■ RTU ■ IED ■ Servers
Software		Applications used to manage the process.	■ SCADA ■ Operating systems ■ Firmware ■ Development tools
Staff		Staff working in the organisation.	■ Permanent ■ Sub-contracted

Asset		Description	Examples
Information		Data that is generated, collected, managed, transmitted and destroyed, regardless of its format.	■ Databases ■ Documentation ■ Manuals
Network		Network connectivity devices.	■ Routers ■ Switches ■ Firewalls
Technology		Equipment needed to manage people the company's and business.	■ Computers ■ Telephones ■ Printers ■ Wiring

INCIBE-CERT. Guide for an asset inventory management in industrial control systems
https://www.incibe-cert.es/en/publications/guides/guide-asset-inventory-management-industrial-control-systems

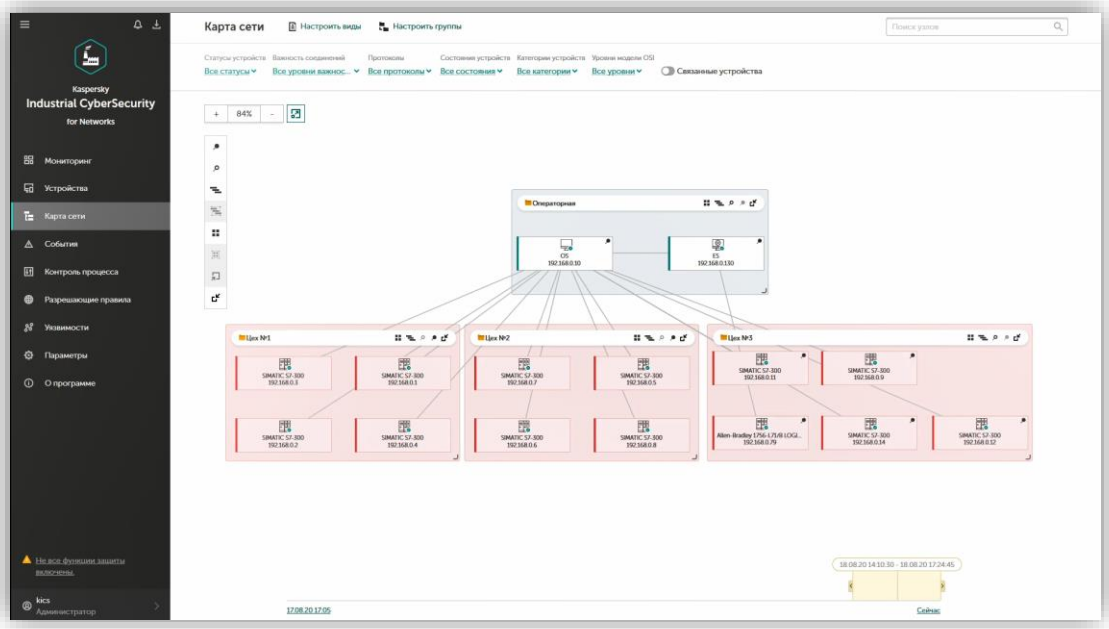
Инструменты инвентаризации активов

Бесплатные и Open Source инструменты



Пример: GRASSMARLIN, Wireshark, Security Onion, NetworkMiner, Nmap, OpenVAS

Коммерческие решения



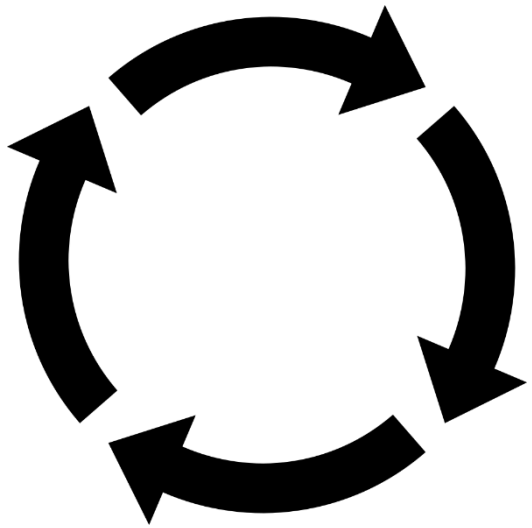
Пример: Kaspersky Industrial CyberSecurity for Networks

Мониторинг изменений и нотификации

- Новые устройства в сети
- Новые уязвимости активов
- Отключения активов от сети
- Аномальные коммуникации активов
- Изменения атрибутов

Система инвентаризации активов будет информировать о всех изменениях активов в промышленном окружении для выявления рисков как можно раньше

Процесс построения инвентаризации



Инвентаризация – непрерывный процесс а не разовый проект!

1. Начните вручную с источникам и документами которые у вас есть, с системами небольшого масштаба

2. Определите атрибуты активов которые вам нужны и для каких целей начните их сбор;

3. Масштабируйте процесс добавляя новые методы инвентаризации (пассивный, активный, анализ конфигурационных файлов) с использованием Open Source коммерческих решений, добавляйте новые атрибуты активов и расширяйте процесс на новые системы;

4. Интегрируйте систему инвентаризации с внешними системами для взаимного обогащения данными и внешней аналитик и представление результатов различным типам пользователей, в т.ч. высшему руководству;

5. Непрерывно поддерживайте процесс инвентаризации.

SANS Institute. ICS Asset Identification: It's More Than Just Security
https://www.sans.org/reading-room/whitepapers/analyst/membership/39650

Поддержка инвентаризации

- Инвентаризация активов должна быть непрерывным процессом
- Частота инвентаризации должна быть как можно выше для оперативного обнаружения изменений
- Частота зависит от типа актива и его атрибутов
- Доступ к результатам инвентаризации активы должен контролироваться и обеспечиваться только авторизованным пользователям
- Результаты инвентаризации активов должны регулярно резервироваться

INCIBE-CERT. Guide for an asset inventory management in industrial control systems
https://www.incibe-cert.es/en/publications/guides/guide-asset-inventory-management-industrial-control-systems

Выгоды для бизнеса

Качественная инвентаризация активов помогает организации лучше понимать и управлять кибер рисками

Инвентаризация активов поддерживает не только цели кибербезопасности, но цели бизнеса, такие как снижение затрат и увеличение прибыли:

1. Наличие **детального актуального реестра активов позволяет восстанавливать операции быстрее**, снижение среднего времени на восстановление работы (MTTR) минимизирует потери в результате остановки, тем самым повышая производительность и прибыль. Один день отсутствия простоя может компенсировать все затраты программу инвентаризации активов

1. Четкий процесс инвентаризации активов может оперативно **обнаруживать активы требующие обслуживания, ремонта или замены**, задолго до того как они негативно повлияют на промышленные процессы. Повышает среднее время до отказа

2. Инвентаризация активов помогает в понимании компонент участвующих в технологических процессах, что **способствует обеспечению безопасного и надежного производства**

3. Качественная инвентаризация активов может **снизить риск регуляторов** связанный с активами на предприятии, которые не соответствуют требованиям регулятора

4. **Начальные инвестиции в инвентаризацию активов могут быть небольшими**, с небольшим масштабом и использованием Open Source решений

5. Инвестиции в автоматизированные решения снижают затраты на ручной труд

SANS Institute. ICS Asset Identification: It's More Than Just Security
https://www.sans.org/reading-room/whitepapers/analyst/membership/39650

Выводы

1. Инвентаризация активов важный и первостепенный шаг обеспечении безопасного и надежного технологического процесса

2. Существующие подходы к инвентаризации включаю: **ручная, активная, пассивная и анализ конфигурационных файлов**. Все подходы имеют свои плюсы и минусы, поэтому для успешного процесса инвентаризации рекомендуется комбинировать подходы

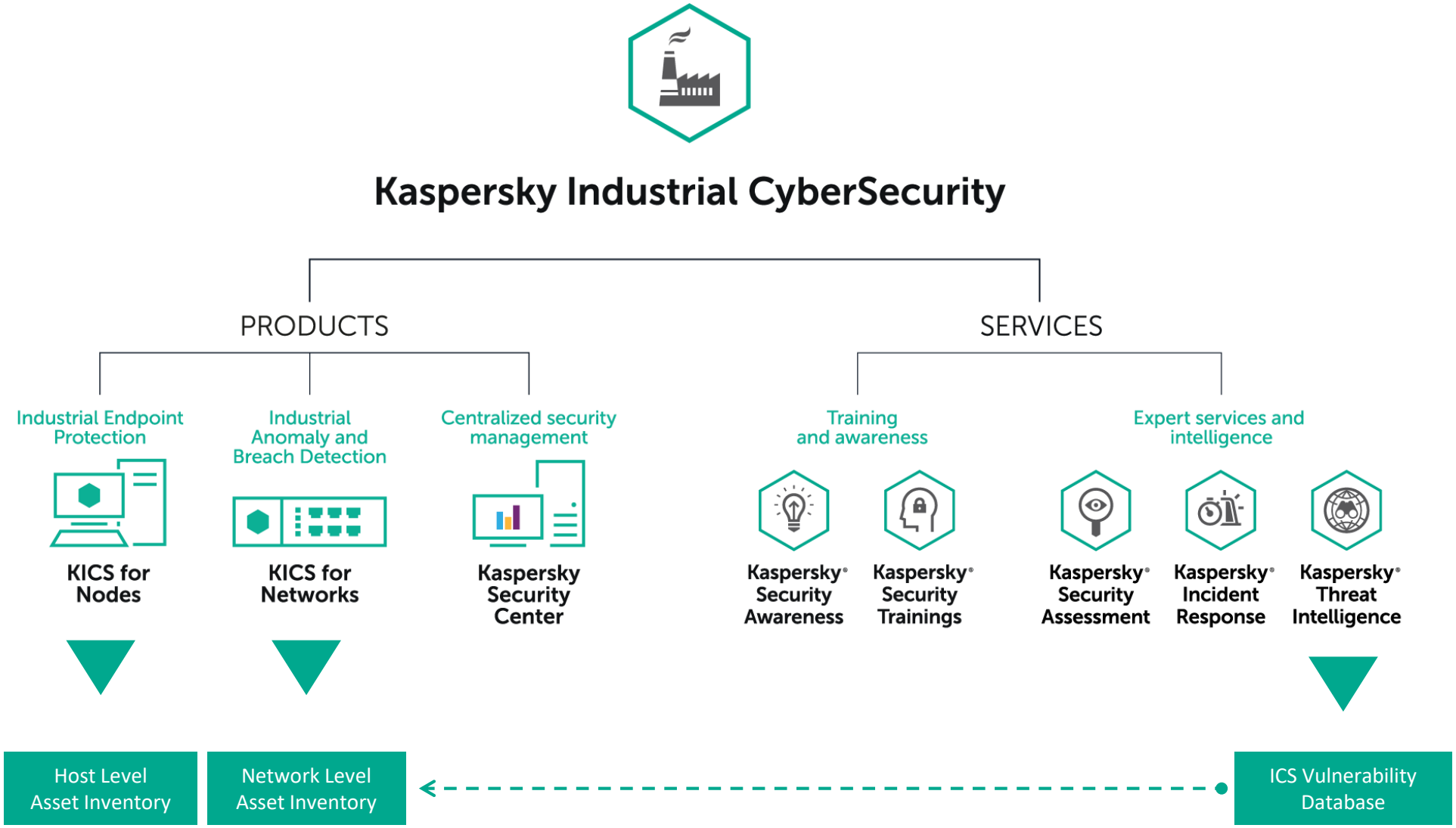
3. Инвентаризация активов не обязательно сложный затратный процесс, начните с малого и развивайте

4. Инвентаризация активов это не только инструмент кибербезопасности, это помощь в снижении время на восстановление и бизнес рисков

5. Для получения ресурсов для программы инвентаризации активов, продемонстрируйте руководству пользу программы для снижения затрат и повышения надежности и функциональной безопасности производства

Источники

1. **Приказ ФСТЭК России №239 «Об утверждении Требований по обеспечению безопасности ЗО КИИ РФ»**
   https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239
2. **INCIBE-CERT. Guide for an asset inventory management in industrial control systems**
   https://www.incibe-cert.es/en/publications/guides/guide-asset-inventory-management-industrial-control-systems
3. **NCCoE, NIST Cybersecurity Practice Guide, SP 1800-23, Energy Sector Asset Management.**
   https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management
4. **SANS Institute. ICS Asset Identification: It's More Than Just Security**
   https://www.sans.org/reading-room/whitepapers/analyst/membership/39650
5. **SANS Institute. Practical ICS Cybersecurity: IT and OT Have Converged - Discover and Defend Your Assets**
   https://www.sans.org/reading-room/whitepapers/analyst/membership/38620
6. **Operational Technology Cyber Security Alliance (OTCSA). Vulnerability Management for Operational Technology**
   https://otcsalliance.org/vulnerability-management/
7. **Center for Internet Security CIS Controls Version 7 Implementation Guide for Industrial Control Systems**
   https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/
8. **AuditScripts Critical Security Control Master Mappings v7.0d**
   https://www.auditscripts.com/?attachment_id=4011
9. **NIST Cybersecurity Framework Version 1.1**
   https://www.nist.gov/cyberframework/framework
10. **NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security**
    https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final



ics.kaspersky.com

kaspersky

Спасибо!

Anton Shipulin, *CISSP, CEH, CSSA*
Anton.Shipulin@kaspersky.com
@shipulin_anton

Kaspersky Industrial Cybersecurity Conference 2020


НУ ПО ГЛАЗАМ ЖЕ ВИЖУ,
ЧТО ЖДЕТЕ!