Принцип Парето в информационной безопасности

Алексей Лукацкий
Бизнес-консультант по безопасности

22 марта 2018

Хакеры украли более 10% всех привлеченных через ICO средств

Зачем нам кибербезопасность?

- А нам нужна ИБ?
- Что мы защищаем?
- По чьему требованию мы защищаем?
- От чего мы защищаем?
- Почему мы защищаем?

Почему организации думают об ИБ?

- Самая популярная причина «продажи» ИБ (реальные инциденты, мифические угрозы, результаты аудита)
- В условиях кризиса не всегда работает (есть более приоритетные риски и угрозы – девальвация, колебания курса, нет заимствований, сокращение, урезание бюджетов…)

- Очень редко когда применяется в ИБ
- В условиях кризиса приобретает очень важное значение

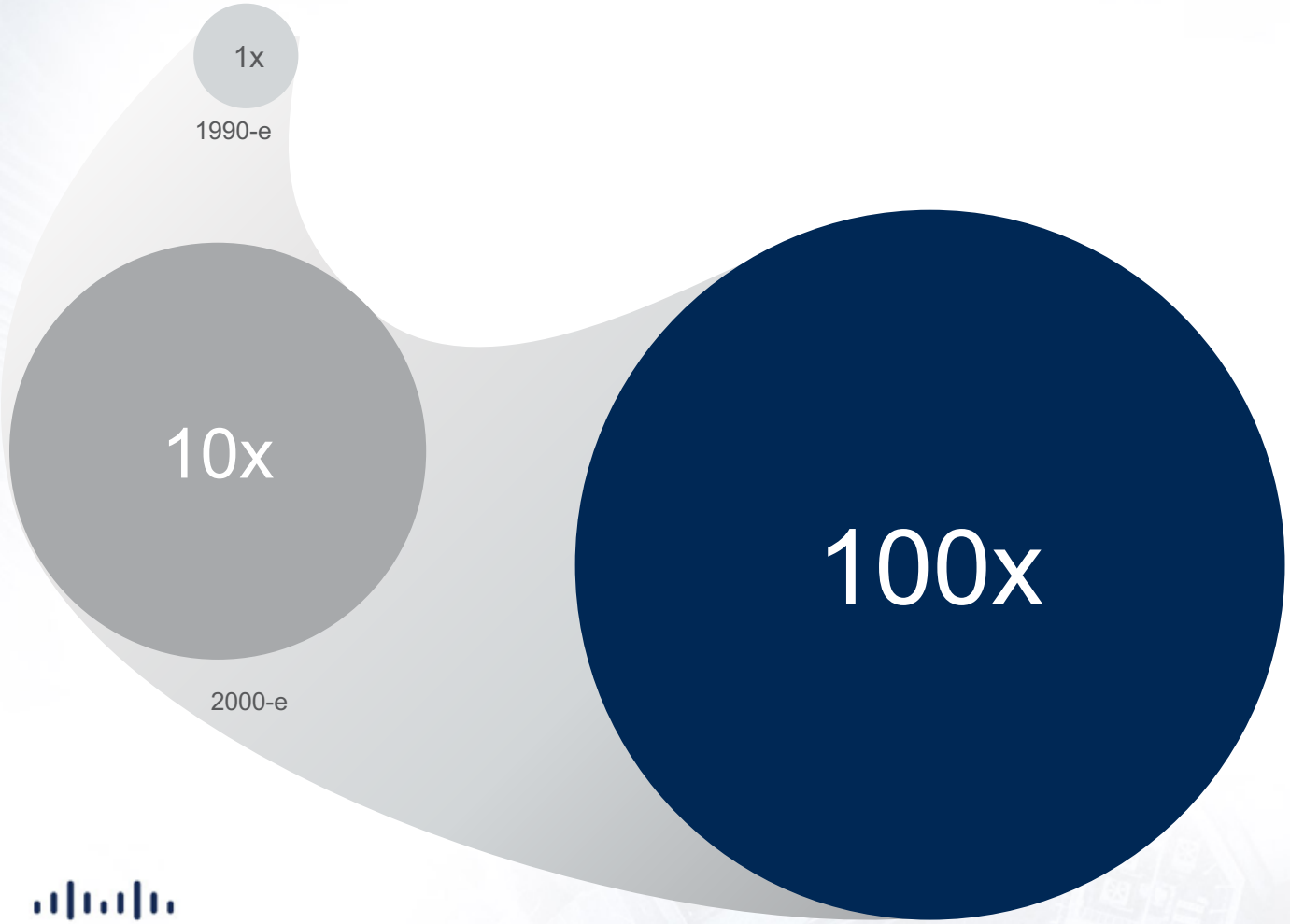
- Наиболее актуальная причина для государственных органов
- Средняя актуальность – крупные предприятия
- Низкая актуальность – средний бизнес
- Практически неактуальна – для малого бизнеса

cisco

Как это делается сейчас

- «О, а вы знаете, что ФСТЭК 4 месяца назад выпустила новый приказ с требованиями по защите? Пойду поищу в Интернете текст»
- «Вот сейчас закончим внедрять СТО БР ИББС и посмотрим в сторону 382-П»
- «Зачем мне читать сам приказ, я у Лукацкого выжимку прочту и все»
- «Я не могу все это реализовать – десятки документов от разных регуляторов с сотнями конфликтующих требований»
- «Дождусь проверки регулятора и будь, что будет»

Взрывной рост числа нормативных актов



Как в них разобраться?

Только один пример - ФСТЭК

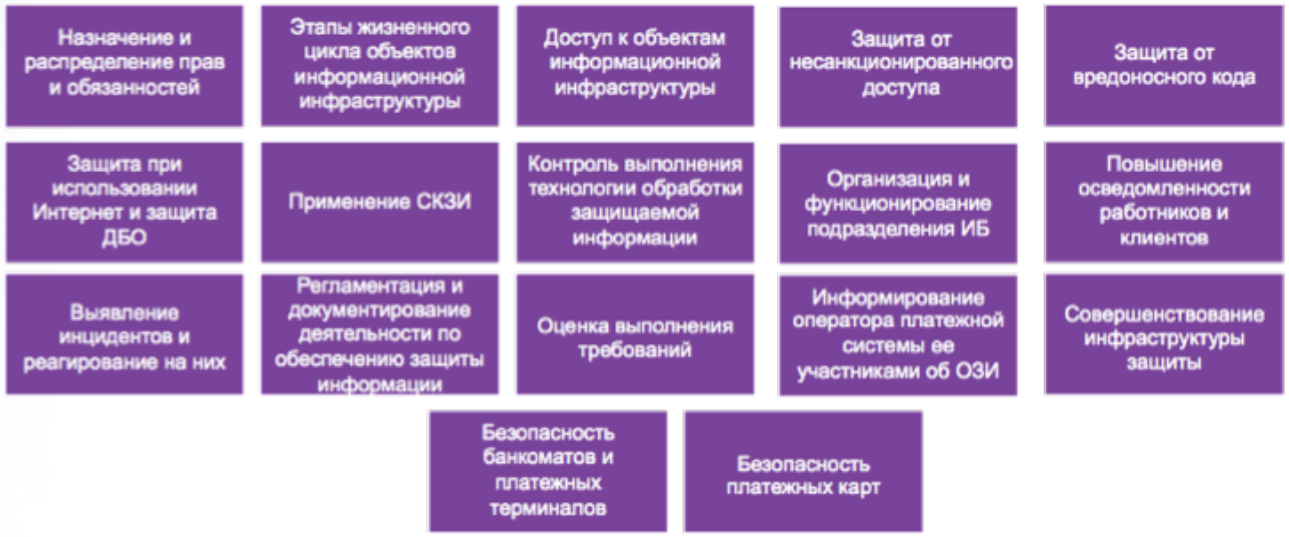
Большое количество требований не позволяет реализовать их последовательно. Особенно в контексте появления новых требований и вовлечения новых регуляторов

Есть ли единый список требований по защите?

Сколько вы знаете НПА с требованиями по ИБ?

Структура системы нормативных правовых актов по ИБ

Сотни требований по защите

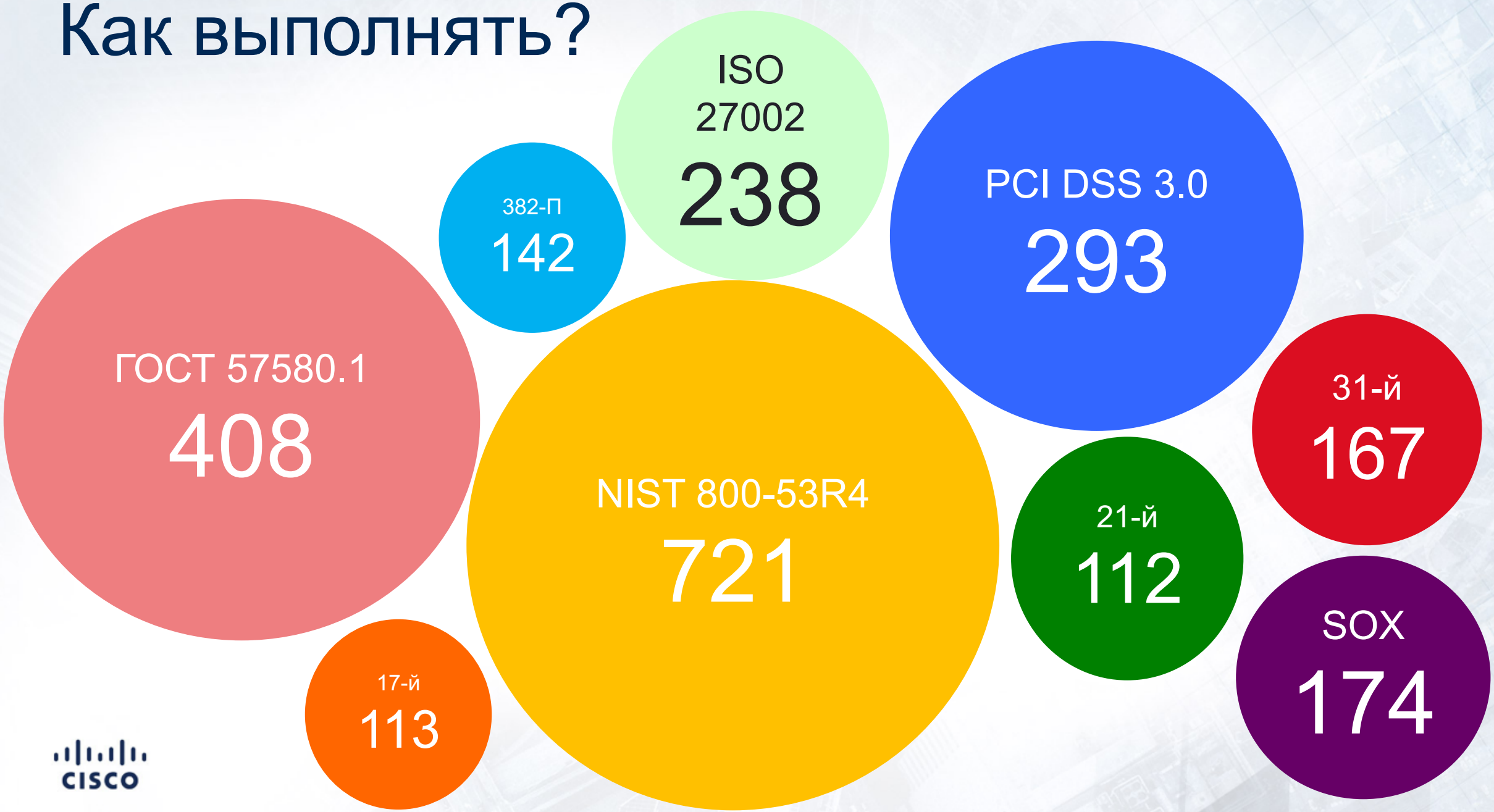


150+ требований в 382-П

№		Меры защиты	Классы защищенности ИС (Приказ 17)				Уровни защищенности ПДн (Приказ 21)				Класс защищенности АСУ		
			4	3	2	1	4	3	2	1	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)													
1.	ИАФ.0	Разработка правил и процедур (политик) идентификации и аутентификации субъектов доступа и объектов доступа	отсутствует				отсутствует				+	+	+
2.	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+	+	+	+	+	+	+	+
3.	ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+			+	+		+	+
4.	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+	+	+	+	+	+	+	+
5.	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+	+	+	+	+	+	+	+
6.	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+	+	+	+	+	+	+	+
7.	ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+	+	+	+	+	+	+	+
8.	ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа					отсутствует						
II. Управление доступом субъектов доступа к объектам доступа (УПД)													
9.	УПД.0	Разработка правил и процедур (политик) управления доступом субъектов доступа к объектам доступа	отсутствует				отсутствует				+	+	+
10.	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+	+	+	+	+	+	+	+
11.	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+	+	+	+	+	+	+	+
12.	УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами			+	+	+	+	+	+	+	+	+

167 требований в 17/21/31-м приказах ФСТЭК

Как выполнять?



Меры по защите информации ФСТЭК

Защитная мера	ПДн	ГИС	АСУ ТП
Идентификация и аутентификация субъектов доступа и объектов доступа	+	+	+
Управление доступом субъектов доступа к объектам доступа	+	+	+
Ограничение программной среды	+	+	+
Защита машинных носителей информации, на которых хранятся и (или) обрабатывается КИ	+	+	+
Регистрация событий безопасности	+	+	+
Антивирусная защита	+	+	+
Обнаружение (предотвращение) вторжений	+	+	+
Контроль (анализ) защищенности персональных данных	+	+	+
Обеспечение целостности информационной системы и КИ	+	+	+
Обеспечение доступности персональных данных	+	+	+
Защита среды виртуализации	+	+	+
Защита технических средств	+	+	+
Защита информационной системы, ее средств, систем связи и передачи данных	+	+	+

Меры по защите информации ФСТЭК

Защитная мера	ПДн	ГИС	АСУ ТП
Управление инцидентами	+		+
Управление конфигурацией информационной системы и системы защиты КИ	+		+
Безопасная разработка прикладного и специального программного обеспечения разработчиком			+
Управление обновлениями программного обеспечения			+
Планирование мероприятий по обеспечению защиты информации			+
Обеспечение действий в нештатных (непредвиденных) ситуациях			+
Информирование и обучение пользователей			+
Анализ угроз безопасности информации и рисков от их реализации			+

- Планы ФСТЭК

  Унификация перечня защитных мер для всех трех приказов

Малоизвестные документы ФСТЭК

- Коммерческая тайна
  - Методические рекомендации по технической защите информации, составляющей коммерческую тайну
- Ключевые системы информационной инфраструктуры
  - Методика определения актуальных угроз безопасности информации в ключевых системах информационных инфраструктурах
  - Общие требования по обеспечению безопасности информации в ключевых системах информационных инфраструктурах
  - Базовая модель угроз безопасности информации в ключевых системах информационных инфраструктурах
  - Рекомендации по обеспечению безопасности информации в ключевых системах информационных инфраструктурах

Малоизвестные документы ISO

- ISO Guide 73. Risk management - Vocabulary - Guidelines for use in standards
- ISO 10181-7. Security audit and alarm framework
- ISO 13569. Banking and related financial services — Information security guidelines
  - Принят как ГОСТ Р ИСО/МЭК
- ISO 15489. Information and Documentation – Records management
- ISO TR 17944. Banking - Security and other financial services - Framework for security in financial systems
- ISO 18043. Selection, deployment and operations of intrusion detection systems

Малоизвестные документы ISO

- ISO 18028. IT network security
- ISO 18044. Security Incident Management
  - Принят как ГОСТ Р ИСО/МЭК
- ISO 18045. Methodology for IT security evaluation
  - Принят как ГОСТ Р ИСО/МЭК
- ISO TR 19791. Security assessment of operational systems
- ISO 21827. Systems Security Engineering — Capability Maturity Model (SSE-CMM)
- ISO 24762. Security techniques — Guidelines for information and communications technology disaster recovery services

Малоизвестные проекты ISO

- ISO 31000. Risk management — Guidelines on principles and implementation of risk management
- Новая серия 270xx
  - ISO 27031 (существенно расширенный) = X.1051
  - ISO 27011 = ISO 27002 для операторов
  - ISO 27012 = ISO 27002 для e-government
  - ISO 27033 (7 частей) = ISO 18028
  - ISO 27034 – application security
  - ISO 27037 = ISO 27002 (взаимодействие государства и бизнеса)
- Новая серия 290xx
  - Privacy Framework, Access Management Framework, Responsible Vulnerability Disclosure, Verification of cryptographic protocols…

BSI или BSI?

- BSI
  - British Standards Institution
  - Bundesamt für Sicherheit in der Informationstechnik
- BSI Standard 100-1 Information Security Management Systems (ISMS)
- BSI-Standard 100-2: IT-Grundschutz Methodology
- BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz

Стандарты ITU-T для операторов связи

- Базовый уровень информационной безопасности операторов связи
- X.805 Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами
- X.1051 Система управления информационной безопасностью – Требования к электросвязи (ISMS-T)
- E.408 Требования к безопасности сетей электросвязи
- E.409 Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи

Стандарты ITU-T для операторов связи

- X.800 Open Systems Security Architecture
- X.802 Lower Layers Security Model
- X.803 Upper Layers Security Model
- X.810 Security frameworks for open systems: Overview
- X.811 SFfOS: Authentication framework
- X.812 SFfOS: Access control framework
- X.813 SFfOS: Non-repudiation framework
- X.814 SFfOS: Confidentiality framework
- X.815 SFfOS: Integrity framework
- X.816 SFfOS: Security audit and alarms framework

Стандарты ITU-T для операторов связи

- G.841 и G.842 – защитные архитектуры SDH
- H.233-H.235 – безопасность мультимедийных служб (например, H.323)
- M.3016 – безопасность сети управления электросвязью
- T.36 – безопасность факсимильной передачи
- X.736 – оповещение о нарушениях безопасности
- X.740 – журнал регистрации событий безопасности
- X.830-X.835 – набор рекомендаций по созданию протоколов высших уровней (согласно OSI) для реализации услуг безопасности
- X.1121 – безопасность мобильной связи

Малоизвестные ГОСТы

- ГОСТ Р 51188-98. Испытания программных средств на наличие компьютерных вирусов
- ГОСТ Р 51583-2000. Порядок создания автоматизированных систем в защищенном исполнении
- ГОСТ Р 51624-2000. Автоматизированные системы в защищенном исполнении
- ГОСТ Р 52448-2005. Обеспечение безопасности сетей электросвязи
- ГОСТ Р 52447-2005. Техника защиты информации. Номенклатура показателей качества

Малоизвестные ГОСТы

- ГОСТ Р 51901.2-2005 (МЭК 60300). Менеджмент риска
  - 16 частей (сейчас опубликованы не все)
- ГОСТ Р 51275-2006. Факторы, воздействующие на информацию
- И еще около шести десятков ГОСТов по информационной безопасности

Другие малоизвестные документы

- HB 174-2003. Information security management - Implementation guide for the health sector
- Generally Accepted Information Security Principles (GAISP)
- Information Security Risk Assessment Practices of Leading Organizations (от US GAO)
- The Standard of Good Practice for Information Security (от ISF)
- Information Security Management Maturity Model (ISM3)
- Свыше сотни документов NIST

Стандарты управления рисками

- AS/NZS 4360
- HB 167:200X
- EBIOS
- ISO 27005 (ISO/IEC IS 13335-2)
- MAGERIT
- MARION
- MEHARI
- CRISAM
- OCTAVE
- ISO 31000
- NIST SP 800-3
- SOMAP
- Lanifex Risk Compass
- Austrian IT Security Handbook
- на основе CRAMM
- A&K Analysis
- ISF IRAM (включая SARA, SPRINT)
- OSSTMM RAV
- BSI 100-3

Настройки оборудования

- Cisco Security Architecture for Enterprise (SAFE)
- Security Configuration Benchmarks (от CIS)
- Router Security Configuration Guide (от NSA)

Как выполнить тысячи требований?

Что же делать?

«Небольшая доля причин, вкладываемых средств или прилагаемых усилий, отвечает за большую долю результатов, получаемой продукции или заработанного вознаграждения»

Вильфредо Парето (1848 – 1923)

Принцип Парето на практике

- 20% вложенных средств ответственны за 80% отдачи
- 80% следствий проистекает из 20% причин
- 20% покупателей приносит 80% прибыли
- 20% преступников совершают 80% преступлений
- 20% водителей виновны в 80% ДТП
- 80% времени вы носите 20% имеющейся одежды
- 80% энергии двигателя теряется впустую
- 20% населения владеют 80% всех ценностей
- 80% времени ПК тратится на 20% команд программы

Суть принципа Парето

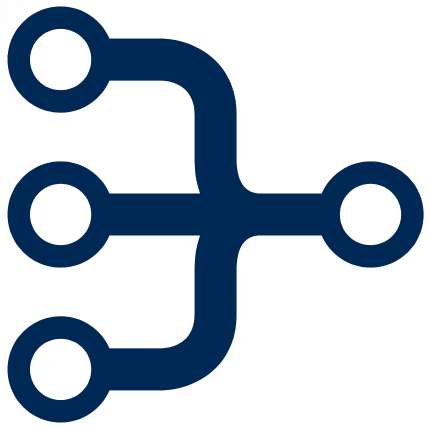
- Диспропорция является неотъемлемым свойством соотношения между причинами и результатами, вкладом и возвратом, усилиями и вознаграждением за них
  - Если мы изучим и проанализируем два набора данных, относящихся к причинам и результатам, то скорее всего получим картину несбалансированности
  - 65/35, 70/30, 75/25, 80/20, 95/5…
- Он опровергает логическое предположение, что все факторы имеют примерно одинаковое значение
- Принцип 80/20 будет работать всегда и везде, если не прилагать усилий по его преодолению

Принцип Парето в безопасности

- 80% людей совершат НСД, если это не станет известным
- 88% ИТ-специалистов допускают месть работодателю после своего увольнения
- 20% уязвимостей приводят к 80% всех атак
- Атаки обычно направлены на 95% уязвимостей, для которых уже существуют способы устранения
- Только 20% функций СЗИ используются на практике
- Стоимость лицензии на систему защиты составляет около 15-20% от совокупной стоимости владения

cisco

Общие требования по защите



На уровне законов

1. Определение угроз безопасности, анализ уязвимостей и анализ рисков
2. Предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения информации на объекте защиты
3. Недопущение воздействия на тех.средства обработки информации, в результате которого может быть нарушено или прекращено функционирование объекта защиты
4. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации
5. Оценка эффективности принимаемых мер по обеспечению безопасности
6. Учет машинных носителей
7. Обнаружение фактов несанкционированного доступа и принятие мер
8. Восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней
9. Установление правил доступа к информации, а также обеспечением регистрации и учета всех действий, совершаемых с ней
10. Контроль за принимаемыми мерами по обеспечению безопасности
11. Непрерывное взаимодействие с ГосСОПКА
12. Наличие ИБ-подразделения или ответственного сотрудника

cisco

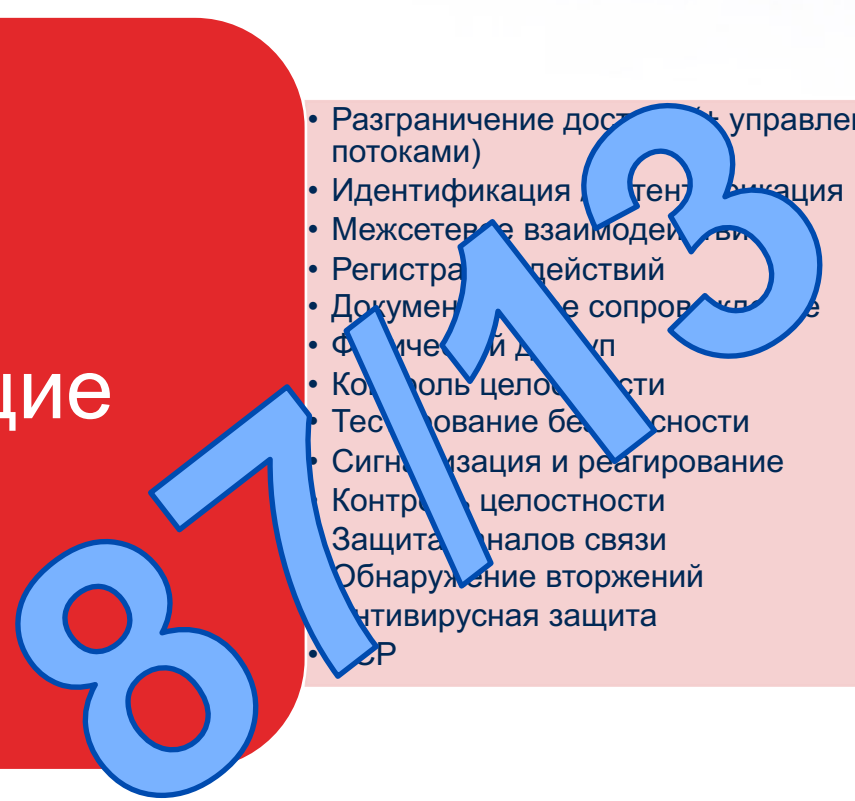
На уровне технических НПА: Россия

Общие

- Разграничение доступа, управление потоками)
- Идентификация и аутентификация
- Межсетевое взаимодействие
- Регистрация действий
- Документирование сопровождение
- Физический доступ
- Контроль целостности
- Тестирование безопасности
- Сигнализация и реагирование
- Контроль целостности
- Защита каналов связи
- Обнаружение вторжений
- Антивирусная защита
- СЗИ

Специфичные

- Защита специфичных процессов (биллинг, АБС, PCI…)
- Защита приложений (Web, СУБД…)
- Нестандартные механизмы (ловушки)



cisco

Топ 4 защитных мер в Австралии

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

October 2012

(U) LEGAL NOTICE: THIS PUBLICATION HAS BEEN PRODUCED BY THE DEFENCE SIGNALS DIRECTORATE (DSD), ALSO KNOWN AS THE AUSTRALIAN SIGNALS DIRECTORATE (ASD). ALL REFERENCES TO ASD SHOULD BE TAKEN TO BE REFERENCES TO DSD.

Top four mitigation strategies to protect your ICT system

1. Targeted cyber intrusions remain the biggest threat to government ICT systems. Since opening in early 2010, the Cyber Security Operations Centre (CSOC) has detected and responded to thousands of these intrusions.

2. You should never assume that your information is of little or no value. Adversaries are not just looking for classified information. A lot of activity observed by the CSOC has an economic focus, looking for information about Australia's business dealings, its intellectual property, its scientific data and the government's intentions.

3. The threat is real, but there are things every organisation can do to significantly reduce the risk of a cyber intrusion. In 2009, based on our analysis of these intrusions, the Australian Signals Directorate produced *Strategies to Mitigate Targeted Cyber Intrusions* – a document that lists a variety of ways to protect an organisation's ICT systems. At least 85% of the intrusions that ASD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the top four mitigation strategies as a package.

4. The top four mitigations are: application whitelisting; patching applications and operating systems and using the latest version; and minimising administrative privileges. This document is designed to help senior managers in organisations understand the effectiveness of implementing these strategies.

Application whitelisting

5. Whitelisting—when implemented correctly—makes it harder for an adversary to compromise an organisation's ICT system. Application whitelisting is a technical measure that only allows specifically authorised applications to run on a system. This helps prevent malicious software and unauthorised applications running.

Patching systems

6. A software patch is a small piece of software designed to fix problems or update a computer program. Patching an organisation's system encompasses both the second and third mitigation strategies. It is important to patch both your operating system and applications within a two-day timeframe for serious vulnerabilities. Once a vulnerability in an operating system or application is made public, you can expect malware to be developed by adversaries within 48 hours. In some cases, malware has been developed to take advantage of a publicly disclosed vulnerability within eight hours.

7. There is often a perception that by patching a system without rigorous testing, something is likely to break on the system. In the majority of cases patching will not affect the function of an organisation's ICT system. Balancing the risk between taking weeks to test patches and patching serious vulnerabilities within a two-day timeframe can be the difference between a compromised and a protected system.

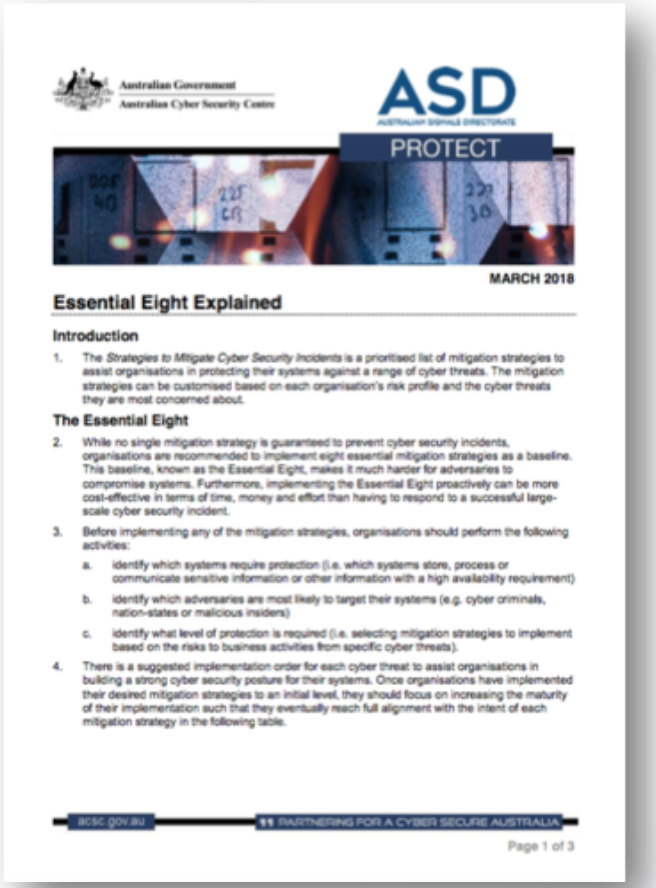
Page 1 of 2

1. Application whitelisting (замкнутая программная среда)
2. Обновление приложений (установка патчей)
3. Обновление операционных систем
4. Ограничение административных привилегий

Закрывают 85% всех угроз

cisco

Топ 8 защитных мер в Австралии



Australian Government
Australian Cyber Security Centre

ASD
AUSTRALIAN SIGNALS DIRECTORATE

PROTECT

MARCH 2018

Essential Eight Explained

Introduction

1. The *Strategies to Mitigate Cyber Security Incidents* is a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of cyber threats. The mitigation strategies can be customised based on each organisation's risk profile and the cyber threats they are most concerned about.

The Essential Eight

2. While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems. Furthermore, implementing the Essential Eight proactively can be more cost-effective in terms of time, money and effort than having to respond to a successful large-scale cyber security incident.
3. Before implementing any of the mitigation strategies, organisations should perform the following activities:
   a. identify which systems require protection (i.e. which systems store, process or communicate sensitive information or other information with a high availability requirement)
   b. identify which adversaries are most likely to target their systems (e.g. cyber criminals, nation-states or malicious insiders)
   c. identify what level of protection is required (i.e. selecting mitigation strategies to implement based on the risks to business activities from specific cyber threats).
4. There is a suggested implementation order for each cyber threat to assist organisations in building a strong cyber security posture for their systems. Once organisations have implemented their desired mitigation strategies to an initial level, they should focus on increasing the maturity of their implementation such that they eventually reach full alignment with the intent of each mitigation strategy in the following table.

acsc.gov.au | 11 PARTNERING FOR A CYBER SECURE AUSTRALIA

Page 1 of 3

1. Application whitelisting (замкнутая программная среда)
2. Обновление приложений (установка патчей)
3. Конфигурация настроек макросов в MS Office
4. Усиление защиты приложений пользователей (отключение Flash, блокирование Java и скриптов и т.п.)
5. Ограничение административных привилегий
6. Многофакторная аутентификация
7. Обновление операционных систем
8. Ежедневное резервное копирование

cisco

Топ35 защитных мер австралийского ASD

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)		Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Prevent Intrusion Stage 1: Code Execution	Helps Contain Intrusion Stage 2: Network Propagation	Helps Contain Intrusion Stage 3: Data Exfiltration
1	(1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2	(2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3	(3)	**Patch operating system vulnerabilities**. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4	(4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No

Once organisations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, additional mitigation strategies can then be selected to address security gaps until an acceptable level of residual risk is reached.

5	(18)	**User application configuration hardening**, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent	Medium	Medium	Medium	No	Yes	No	No
6	(N/A)	**Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent	Low	Medium	Low	Yes	Yes	No	Possible
7	(21)	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent	Low	Medium	Low	Possible	Yes	Possible	No
8	(11)	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent	Low	Medium	Medium	Yes	Yes	No	Possible
9	(5)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent	Low	Medium	Low	No	No	Yes	No
10	(7)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent	Low	High	Medium	Yes	No	Yes	Possible
11	(6)	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	Excellent	Medium	High	Medium	No	No	Possible	No
12	(8)	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent	Low	Medium	Medium	Yes	Yes	Yes	No
13	(9)	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted application, and denying network traffic by default.	Excellent	Medium	Medium	Medium	Yes	No	Yes	Yes
14	(10)	**Non-persistent virtualised sandboxed trusted operating environment**, hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent	High	High	Medium	Possible	No	Yes	Possible
15	(12)	**Centralised and time-synchronised logging of successful and failed computer events**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
16	(13)	**Centralised and time-synchronised logging of allowed and blocked network activity**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
17	(14)	**Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Yes	Yes	No	Possible
18	(15)	**Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent	Medium	Medium	Medium	Yes	Yes	No	Possible
19	(16)	**Web domain whitelisting for all domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	High	High	Medium	Yes	Yes	No	Yes
20	(19)	**Block spoofed emails** using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low	Low	Low	Possible	Yes	No	No
21	(22)	**Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good	Medium	Medium	Low	Possible	Yes	Yes	Possible
22	(25)	**Antivirus software using heuristics and automated Internet-based reputation ratings** to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good	Low	Low	Low	Yes	Yes	No	No
23	(24)	**Deny direct Internet access from workstations** by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good	Low	Low	Low	Yes	Possible	No	Yes
24	(23)	**Server application configuration hardening** e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good	Low	High	Medium	Possible	Yes	No	Possible
25	(27)	**Enforce a strong passphrase policy** covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.	Good	Medium	Medium	Low	Possible	No	Yes	No
26	(29)	**Removable and portable media control** as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High	Medium	Medium	No	Yes	Possible	Yes
27	(28)	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good	Low	Medium	Low	No	Yes	Yes	No
28	(20)	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good	Medium	High	Medium	Possible	Possible	No	No
29	(26)	**Workstation inspection of Microsoft Office files** for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good	Low	Low	Low	Possible	Yes	No	No
30	(25)	**Signature-based antivirus software** that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.	Good	Low	Low	Low	Possible	Possible	No	No
31	(30)	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good	Low	Low	Low	No	No	No	No
32	(32)	**Block attempts to access websites by their IP address** instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average	Low	Low	Low	Yes	Yes	No	Yes
33	(33)	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low	High	High	Possible	Possible	Possible	Possible
34	(34)	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average	Low	Low	High	Possible	Yes	No	Yes
35	(35)	**Capture network traffic** to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average	Low	High	Low	No	No	No	No

85% угроз

Топ20 защитных мер SANS

- Twenty Critical Security Controls for Effective Cyber Defense от SANS

  В 2015-м году перешли в Center for Internet Security (CIS)

- Динамично обновляемый перечень 20 основных защитных мер против актуальных угроз, построенный по 5 принципам:

  При разработке мер защиты использовалась информация о наиболее актуальных способах атак

  Для каждой меры защиты определен её приоритет; это позволяет в первую очередь внедрять меры, которые уменьшают наиболее опасные риски;

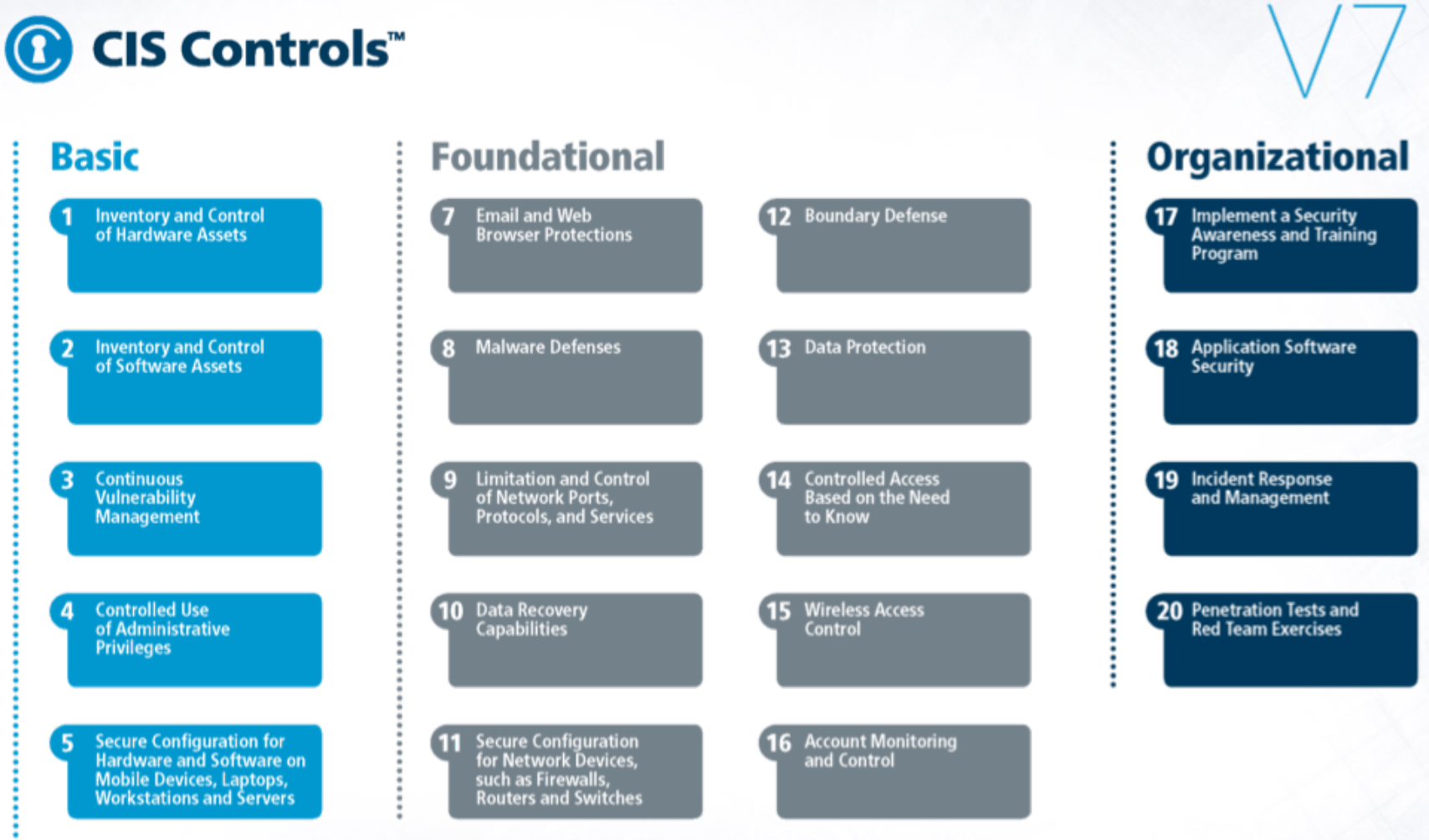
  Эффективность применяемых мер защиты должны быть измеряемой

  Необходимо применять постоянный мониторинг мер защиты

  Там где это возможно необходимо автоматизировать выполнение мер

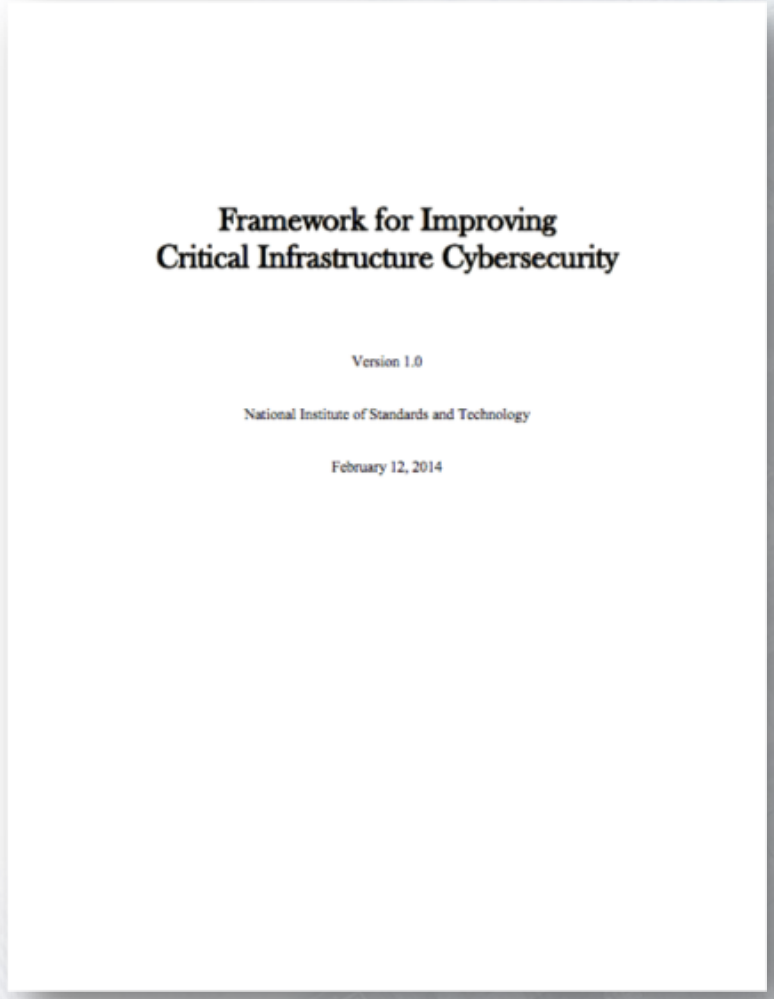
20 Critical Security Controls		National Security Agency Assessment of the 20 Critical Controls			
Critical Security Control	Critical Security Control Description	Tier	Attack Mitigation	Dependencies	Technical Maturity
1 Inventory of Authorized and Unauthorized Devices	**Reduce the ability of attackers to find and exploit unauthorized and unprotected systems:** Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.	1	Very High	Foundational	High
2 Inventory of Authorized and Unauthorized Software	**Identify vulnerable or malicious software to mitigate or root out attacks:** Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.	1	Very High	Foundational	High
3 Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers	**Prevent attackers from exploiting services and settings that allow easy access through networks and browsers:** Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.	1a	Very High	Capability	High
4 Continuous Vulnerability Assessment and Remediation	**Proactively identify and repair software vulnerabilities reported by security researchers or vendors:** Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.	1a	Very High	Capability	High
5 Malware Defenses	**Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading:** Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.	1a	High/ Medium	Capability	High/ Medium
6 Application Software Security	**Neutralize vulnerabilities in web-based and other application software:** Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).	2	High	Capability	Medium
7 Wireless Device Control	**Protect the security perimeter against unauthorized wireless access:** Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.	2	High	Capability	Medium
8 Data Recovery Capability	**Minimize the damage from an attack:** Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.	2	Medium	Capability	Medium
9 Security Skills Assessment and Appropriate Training to Fill Gaps	**Find knowledge gaps, and fill them with exercises and training:** Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.	2	Medium	Capability	Medium
10 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	**Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments:** Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.	3	High/ Medium	Capability/ Dependent	Medium/ Low
11 Limitation and Control of Network Ports, Protocols, and Services	**Allow remote access only to legitimate users and services:** Apply host-based firewalls and port-filtering and -scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.	3	High/ Medium	Capability/ Dependent	Medium/ Low
12 Controlled Use of Administrative Privileges	**Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attacks:** (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.	4	High/ Medium	Dependent	Medium
13 Boundary Defense	**Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines:** Establish multilayered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").	4	High/ Medium	Dependent	Medium/ Low
14 Maintenance, Monitoring, and Analysis of Security Audit Logs	**Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines:** Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.	4	Medium	Dependent	Medium
15 Controlled Access Based on the Need to Know	**Prevent attackers from gaining access to highly sensitive data:** Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.	4	Medium	Dependent	Medium/ Low
16 Account Monitoring and Control	**Keep attackers from impersonating legitimate users:** Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.	4	Medium	Dependent	Medium/ Low
17 Data Loss Prevention	**Stop unauthorized transfer of sensitive data through network attacks and physical theft:** Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.	5	Medium/ Low	Dependent	Low
18 Incident Response Management	**Protect the organization's reputation, as well as its information:** Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	5	Medium	Dependent	Low
19 Secure Network Engineering	**Keep poor network design from enabling attackers:** Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.	6	Low	Indirect	Low
20 Penetration Tests and Red Team Exercises	**Use simulated attacks to improve organizational readiness:** Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems to test existing defenses and response capabilities.	6	Low	Indirect	Low

От SANS Top 20 к CIS Controls



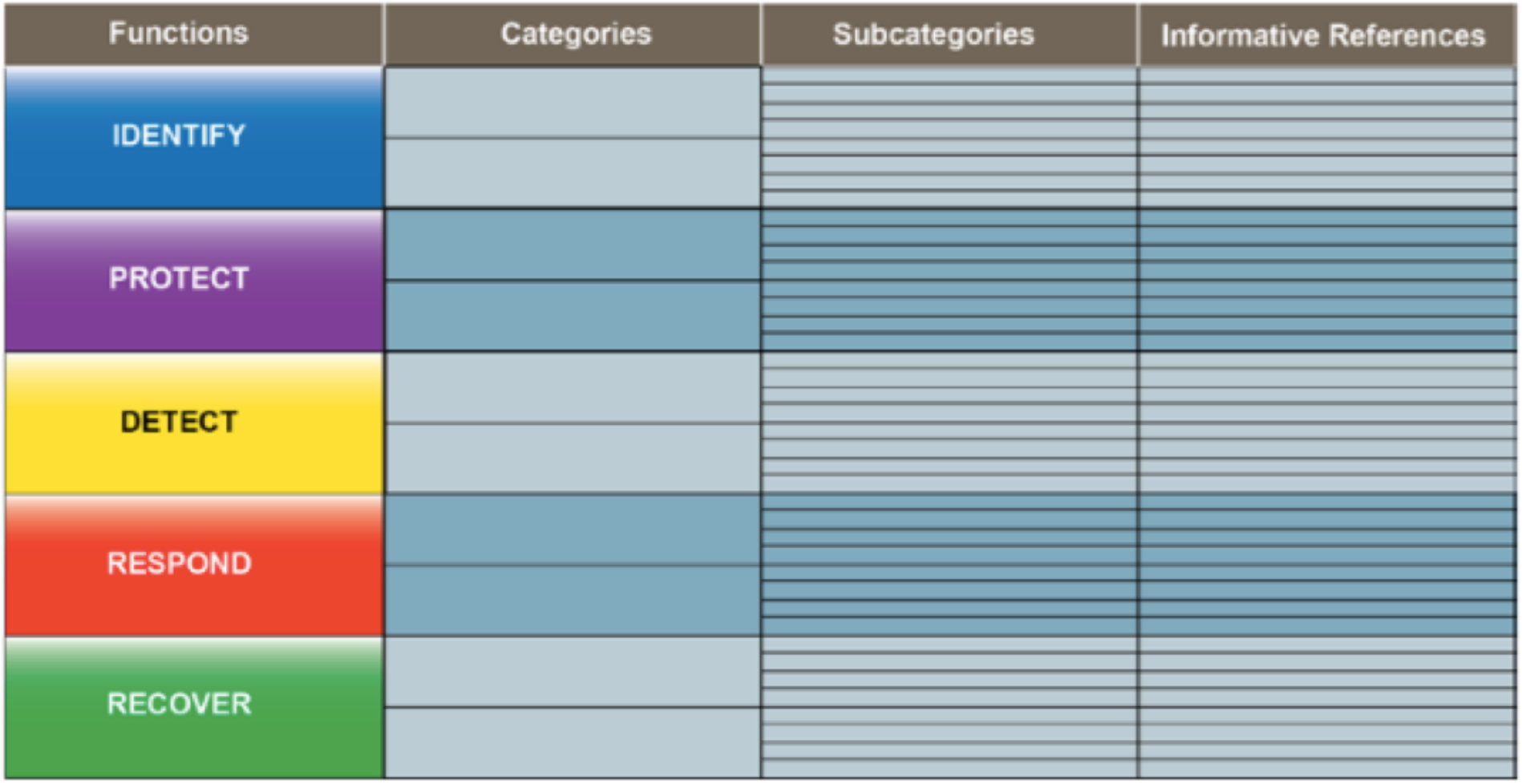
NIST Cybersecurity Framework: последние достижения

- Быть гибкой
- Быть непредписывающей
- Использовать существующие стандарты, подходы и практики
- Быть применимой глобальной
- Фокусировать на управлении рисками, а не выполнении нормативных требований



cisco

Структура Framework



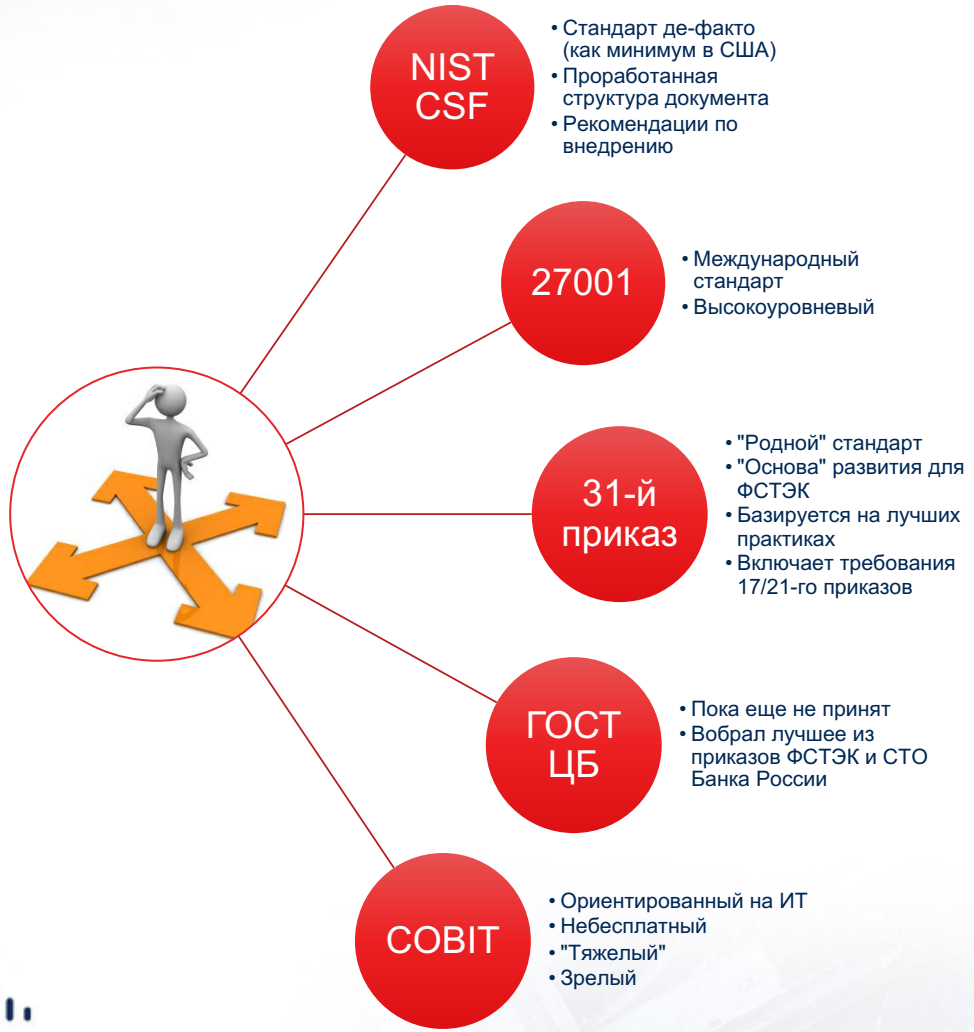
cisco

Защитные меры из NIST CSF

- Стандарты NIST 800-82 и 800-53
- ISA/IEC-62443
- ISO 27001/02
- Стандарты ENISA
- Стандарт Катара
- Стандарт API
- Рекомендации ICS-CERT
- COBIT
- Council on CyberSecurity (CCS)
  Top 20 Critical Security Controls (CSC)

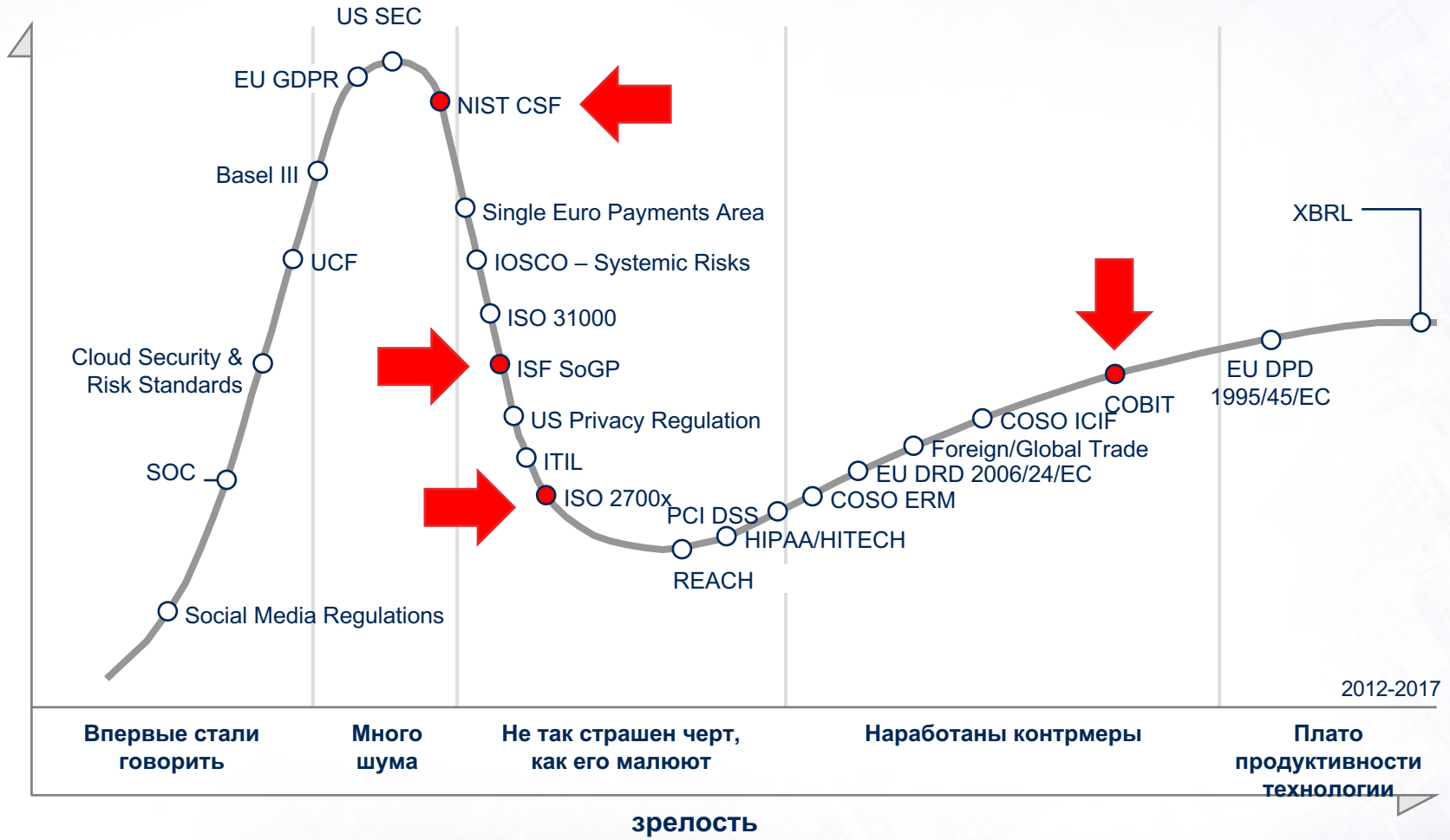
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Что взять за основу?



- Выбор остается за вами – «лучшего» варианта не существует
- Выбор зависит от вашего опыта работы с указанными стандартами и вашей организации (финансы, госы и др.)
- Выполнив основные требования по защите, останется только выполнить формальности

Готовность разных международных НПА

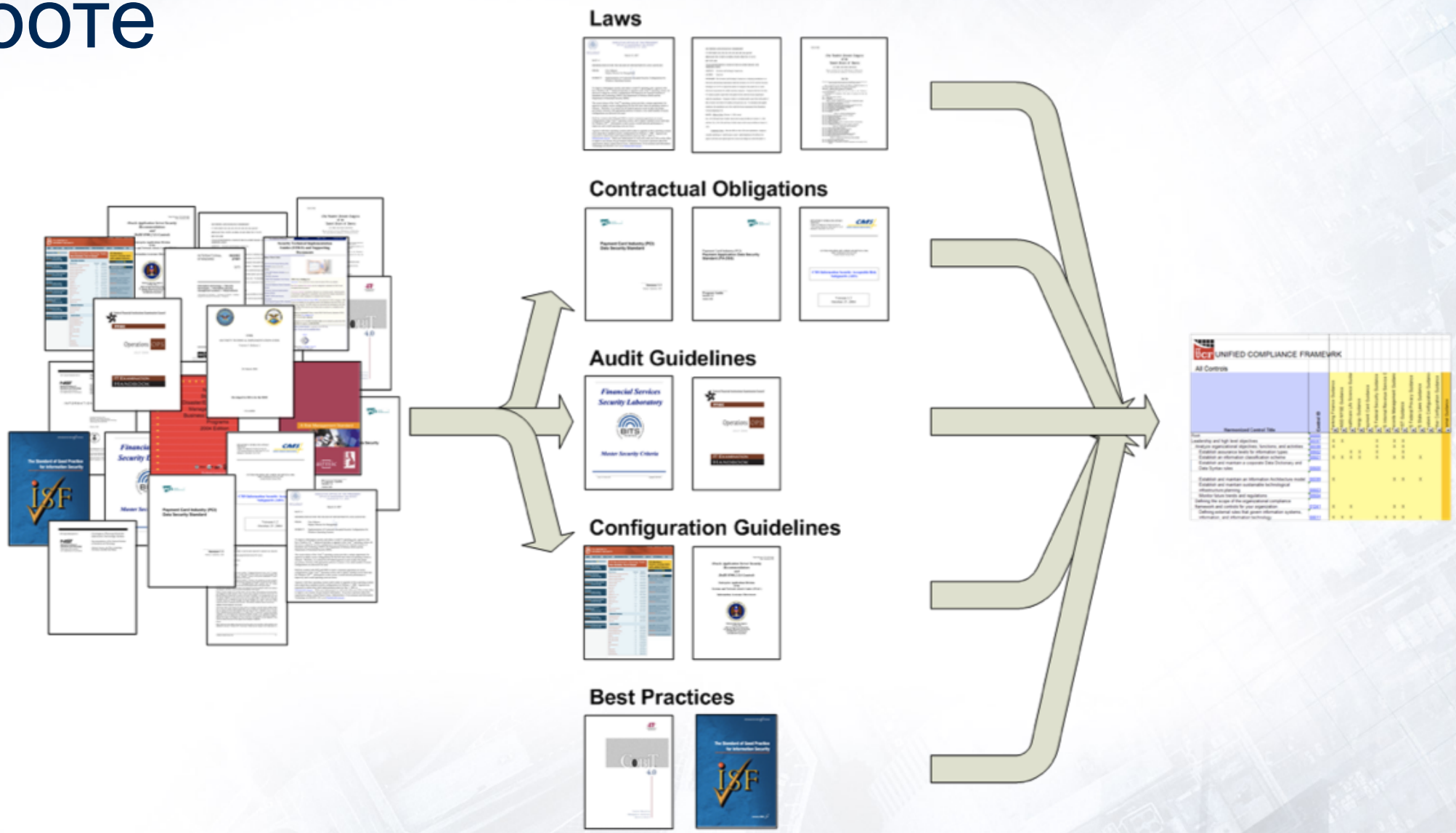


Возможно NIST CSF? Не только ЧТО, но и КАК!

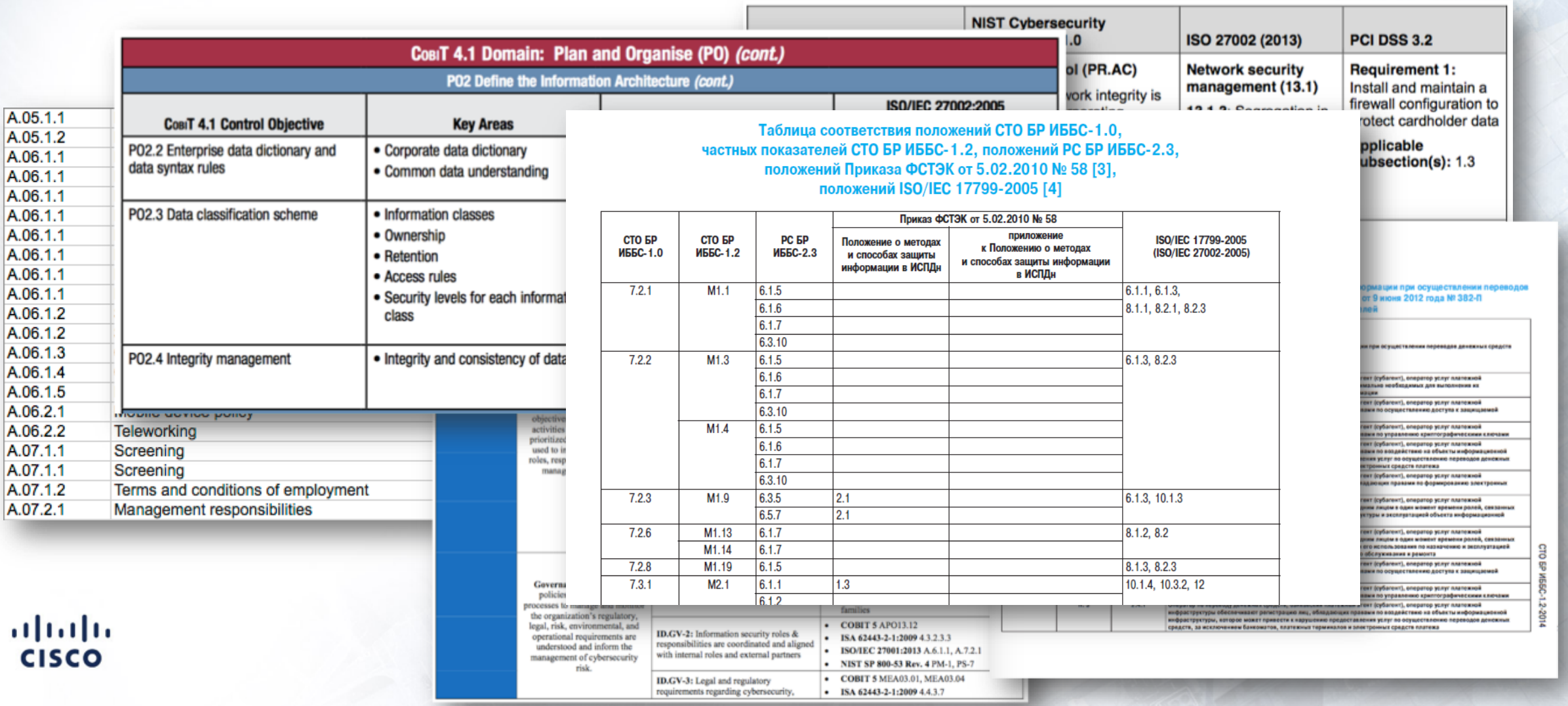
Функция CSF	Категория защитных мер
Идентификация	• Управление активами • Бизнес-окружение • Governance • Оценка рисков • Стратегия управления рисками • Управление цепочками поставок
Защита / Предотвращение	• Контроль и управление доступом и идентификационными данными • Повышение осведомленности & Обучение • Защита данных • Процессы & процедуры защиты данных • Технологии поддержки ИБ • Защитные технологии
Обнаружение	• Аномалии & события безопасности • Непрерывный мониторинг безопасности • Процессы обнаружения
Реагирование	• Планирование реагирования • Коммуникации • Анализ • Нейтрализация • Улучшения
Восстановление	• Планирование восстановления • Улучшения • Коммуникации

cisco

Mapping – очень полезная вещь в работе



Соответствие CSP SCF, PCI DSS, NIST CSF, ISO 27001, COBIT (mapping)



A.05.1.1	
A.05.1.2	
A.06.1.1	
A.06.1.1	
A.06.1.1	
A.06.1.1	
A.06.1.1	
A.06.1.1	
A.06.1.1	
A.06.1.2	
A.06.1.2	
A.06.1.3	
A.06.1.4	
A.06.1.5	
A.06.2.1	
A.06.2.2	Teleworking
A.07.1.1	Screening
A.07.1.1	Screening
A.07.1.2	Terms and conditions of employment
A.07.2.1	Management responsibilities

CobiT 4.1 Domain: Plan and Organise (PO) *(cont.)*

PO2 Define the Information Architecture *(cont.)*

CobiT 4.1 Control Objective	Key Areas	ISO/IEC 27002:2005
PO2.2 Enterprise data dictionary and data syntax rules	• Corporate data dictionary • Common data understanding	
PO2.3 Data classification scheme	• Information classes • Ownership • Retention • Access rules • Security levels for each informat class	
PO2.4 Integrity management	• Integrity and consistency of data	

	NIST Cybersecurity .0	ISO 27002 (2013)	PCI DSS 3.2
	ol (PR.AC) vork integrity is	Network security management (13.1)	Requirement 1: Install and maintain a firewall configuration to rotect cardholder data pplicable ubsection(s): 1.3

Таблица соответствия положений СТО БР ИББС-1.0, частных показателей СТО БР ИББС-1.2, положений РС БР ИББС-2.3, положений Приказа ФСТЭК от 5.02.2010 № 58 [3], положений ISO/IEC 17799-2005 [4]

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
7.2.1	M1.1	6.1.5			6.1.1, 6.1.3, 8.1.1, 8.2.1, 8.2.3
		6.1.6			
		6.1.7			
		6.3.10			
7.2.2	M1.3	6.1.5			6.1.3, 8.2.3
		6.1.6			
		6.1.7			
		6.3.10			
	M1.4	6.1.5			
		6.1.6			
		6.1.7			
		6.3.10			
7.2.3	M1.9	6.3.5	2.1		6.1.3, 10.1.3
		6.5.7	2.1		
7.2.6	M1.13	6.1.7			8.1.2, 8.2
	M1.14	6.1.7			
7.2.8	M1.19	6.1.5			8.1.3, 8.2.3
7.3.1	M2.1	6.1.1	1.3		10.1.4, 10.3.2, 12
		6.1.2			

ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 • NIST SP 800-53 Rev. 4 PM-1, PS-7
ID.GV-3: Legal and regulatory requirements regarding cybersecurity,	• COBIT 5 MEA03.01, MEA03.04 • ISA 62443-2-1:2009 4.4.3.7

СТО БР ИББС-1.2-2014

Не бороться с угрозами, а усложнять жизнь хакерам

- Как усложнить поиск цели?
- Как усложнить проникновение на цель?
- Как усложнить использование цели?
- Как усложнить скрытие атаки?
- Как сделать последствия от атак обратимыми?

THE US-CCU CYBER-SECURITY MATRIX						
	Overview	Harder to Find	Harder to Penetrate	Harder to Co-opt	Harder to Conceal	More Reversible
Hardware						
Software						
Networks						
Automation						
Users						
Suppliers						

cisco

Как защититься от киберугроз?

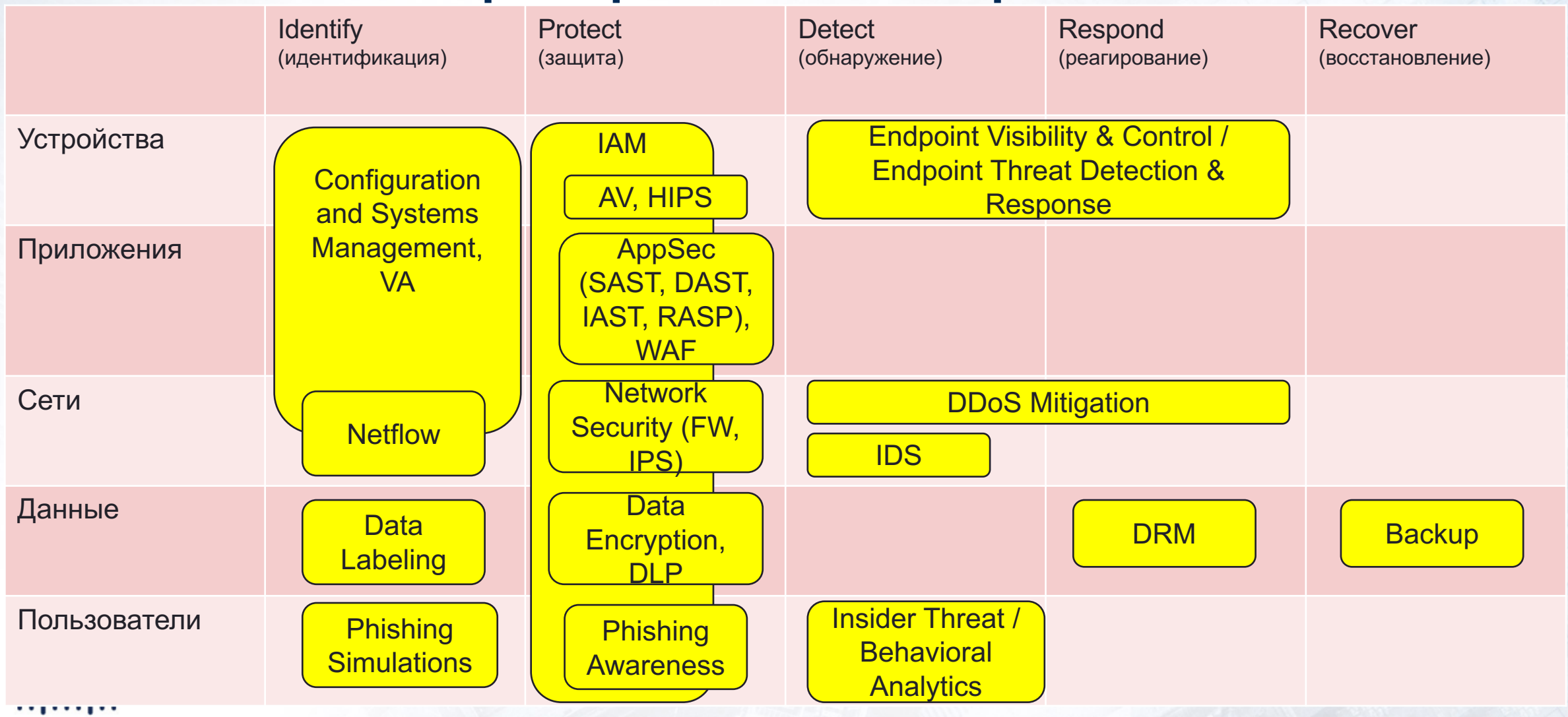
Фаза	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Разведка	Web-аналитика	МСЭ ACL				
Оснастка (вооружение)	NIDS	NIPS				
Доставка	Бдительный пользователь CF	Прокси CF	Inline AV	Управление очередями		
Проникновение	HIDS EDR	Патчи EDR	DEP			
Инсталляция	HIDS EDR	Права доступа EDR	AV			
Управление	NIDS EDR	МСЭ ACL EDR	NIPS		DNS redirect	
Действия на жертве	Логи EDR	HIPS EDR		Качестве обслуживания	Обманная система	

Как все-таки защититься от киберугроз?

	Identify (идентификация)	Protect (защита)	Detect (обнаружение)	Respond (реагирование)	Recover (восстановление)
Сети					
Устройства					
Приложения					
Пользователи					
Данные					

cisco

Сегменты корпоративного рынка ИБ



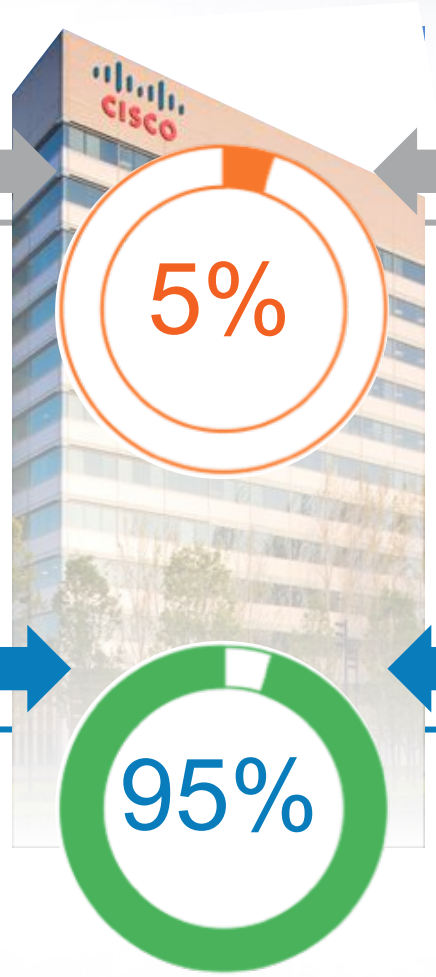
Как это сделано в Cisco?

Продвинутых угроз

- Целевой фишинг с троянами
- Атаки Watering hole
- Атаки через соцсети
- Атаки спецслужб

Расширенные решения

- Расширенный сбор данных
  - Netflow, IP атрибуция, DNS…
- Анализ Big data и playbooks
- Быстрая локализация
  - DNS/RPZ, карантин, On-line форензика на узлах
- Осведомленность об угрозах



Сложности ИБ

- Неуправляемые десктопы и ПК руководства
- Спам/Вредоносное ПО
- DDoS
- Удаленно контролируемые зараженные узлы
- Быстро меняющееся окружение

Базовые решения

- Anti-virus
- Firewalls
- IDS/IPS
- IronPort WSA/ESA
- Сегментация сети (активно развивается)
- Захват и анализ логов
- Incident response team

Как выбрать защитные меры?

Если вам не хватает Топ 4 / Топ 8 / Топ 20 / Топ 35

- Выбор мер по обеспечению безопасности, подлежащих реализации в системе защиты, включает
  - выбор базового состава мер
  - адаптацию выбранного базового набора мер применительно к структурно-функциональным характеристикам ИС, реализуемым ИТ, особенностям функционирования ИС и модели угроз
  - уточнение (включает дополнение или исключение)
  - дополнение адаптированного базового набора мер по обеспечению безопасности дополнительными мерами, установленными иными нормативными актами
- По этому принципу построены документы ФСТЭК, NIST, ISO, SoGP, COBIT, а также ЦБ переходит на него

cisco

Cisco SAFE – это модель

Это действия и противодействия

Это теория игр

Упрощенная, но действенная модель

Мы стартуем с определения актуальных угроз…

С чем мы боремся: угрозы

Примеры

Зомби

DDoS

Пользователи, выдающие себя за других

Перенаправление

Разрушение

Трояны

Черви

Шпионское ПО

Команда и управление

Атаки нулевого дня

Проникновение

Добавление услуг

Просачивание наружу

Шпионские программы

Вирусы

Утечки

…и защищаемся от них

cisco


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
CENTRAL SECURITY SER
UNITED STATES OF AMER
NATIONAL CENTRA
SECURITY SECURIT
D AGENCY SERVIC

Что такое SAFE?

- SAFE снижает сложность
- Игровая модель позволяет упростить общение на одном языке
- Достоверные и проверенные архитектуры и дизайны с базовым уровнем безопасности

cisco

Поэтапное упрощение вопроса обеспечения безопасности

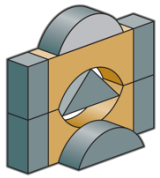
Фаза возможностей

Фаза архитектуры

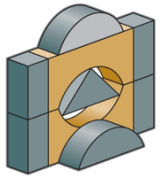
Фаза дизайна

cisco

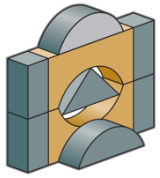
Разбейте сеть на элементы и области



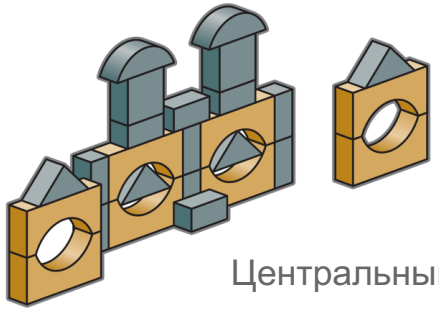
Банкомат



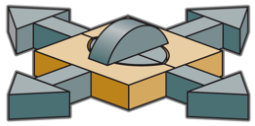
Дочернее предприятие



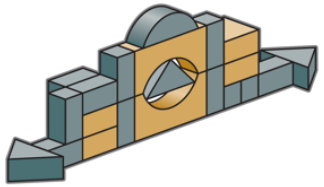
Банк



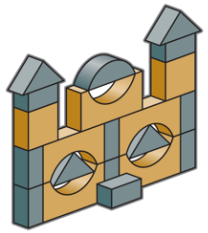
Центральный офис



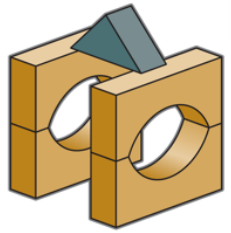
WAN



Интернет-периметр

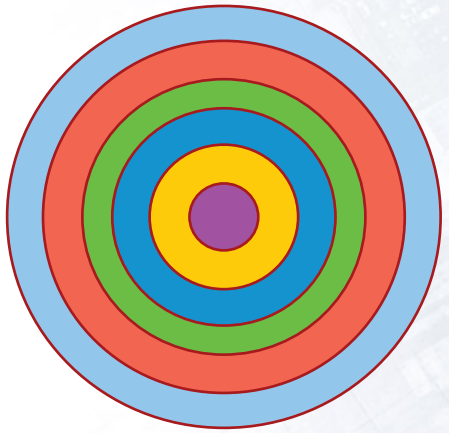


ЦОД



Электронная коммерция

Соответствие требованиям



cisco

С помощью чего мы боремся: возможности


Управление доступом с использованием TrustSec


Анализ/корреляция


Обнаружение аномалий


Анти-вредоносное ПО


Анти-спам


Мониторинг и контроль приложений (AVC)


Безопасность клиента


Cisco Cloud Web Security


Предотвращение утечки данных


База данных


Защита от DDoS-атак


Шифрование электронной почты


Защита электронной почты


Коммутация фабрики


Межсетевой экран


Межсетевой экран


Анализ потока


Идентификация Авторизация


Идентификация Авторизация


Обнаружение вторжений


Предотвращение вторжений


Коммутация L2


Виртуальная коммутация L2


Сеть L2/L3


Сеть L2/L3


Коммутация L3


Балансировщик нагрузки


Регистрация в журнале/ отчетность


Песочница для вредоносного ПО


Управление мобильными устройствами


Мониторинг


Политики/ конфигурация

Возможности

- Говоря о возможностях, мы упрощаем принятие решения, так как внимание фокусируется на функциях защиты, а не на самом продукте или его фичах
- Нам нужен не Cisco ASA или Firepower, нам нужно разграничение сетевого доступа
- У Cisco это может быть решено с помощью
  - Многофункциональных устройств ASA или Firepower
  - Маршрутизатора ISR с IOS Firewall
  - Виртуального МСЭ ASAv или VSG
  - Маршрутизатора ASR с IOS Firewall
  - Облачного МСЭ Meraki
  - Коммутаторов Catalyst 6000 с модулем МСЭ…

Стратегия возможностей

Недоверенные

Проникновение наружу

Черви

Трояны

Шпионское ПО

Угрозы

Место в сети

Доступ

Оценка состояния

Сеть L2/L3

Защита от DDoS-атак

Балансировщик нагрузки

Предотвращение вторжений

Межсетевой экран

Безопасность веб-трафика

МСЭ веб-приложений

Политики/ конфигурация

Анализ/ корреляция

Мониторинг и контроль приложений (AVC)

Регистрация в журнале/ отчетность

Мониторинг

Управление уязвимостями

Совместно используемые

Доверенные

Сервер

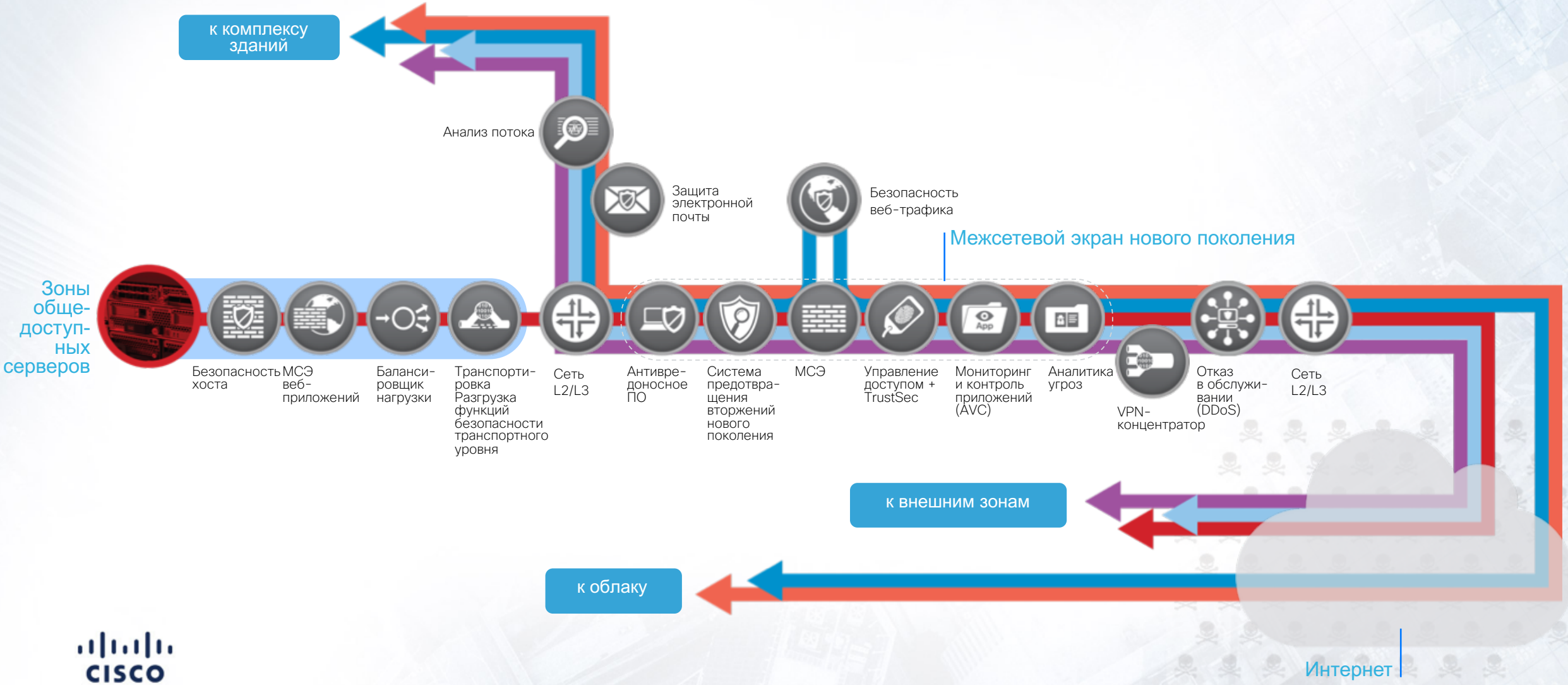
Хранение

База данных

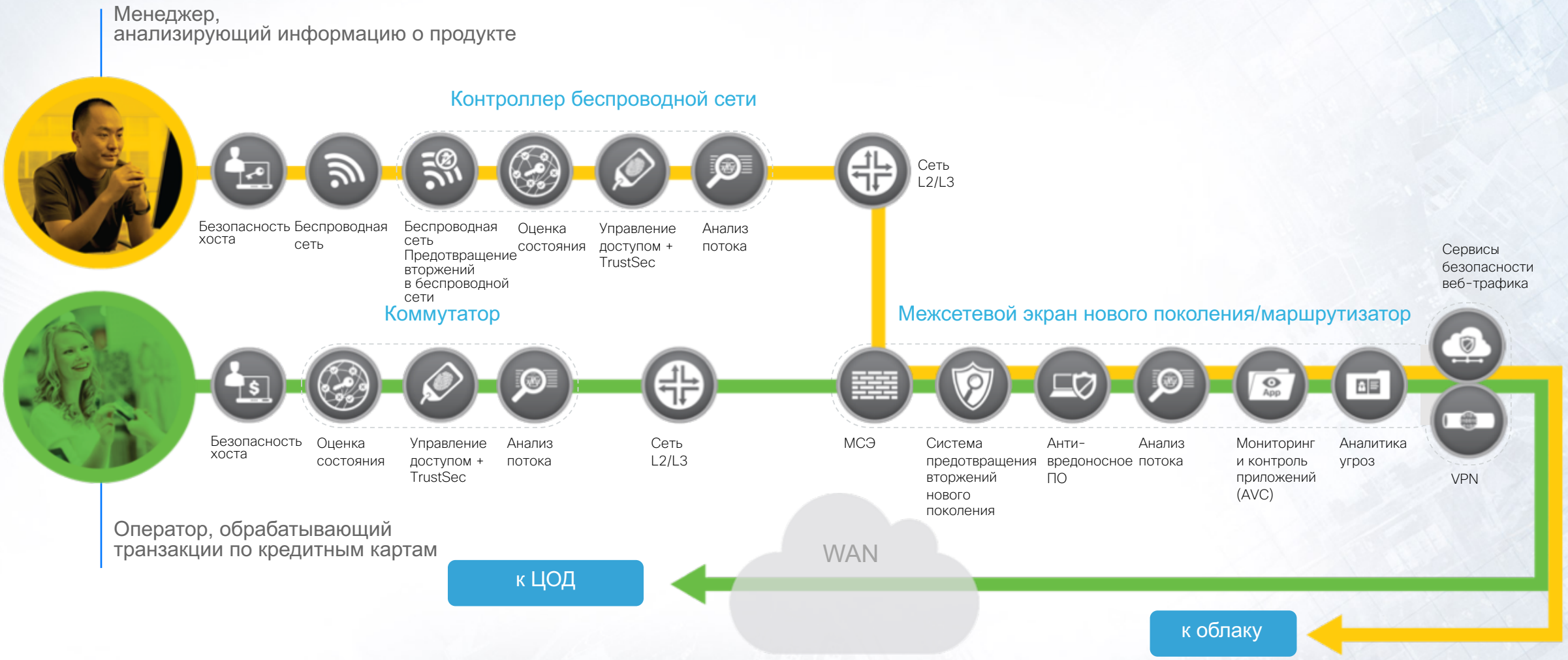
Приложение

Сервисы

SAFE упрощает обеспечение ИБ: периметр

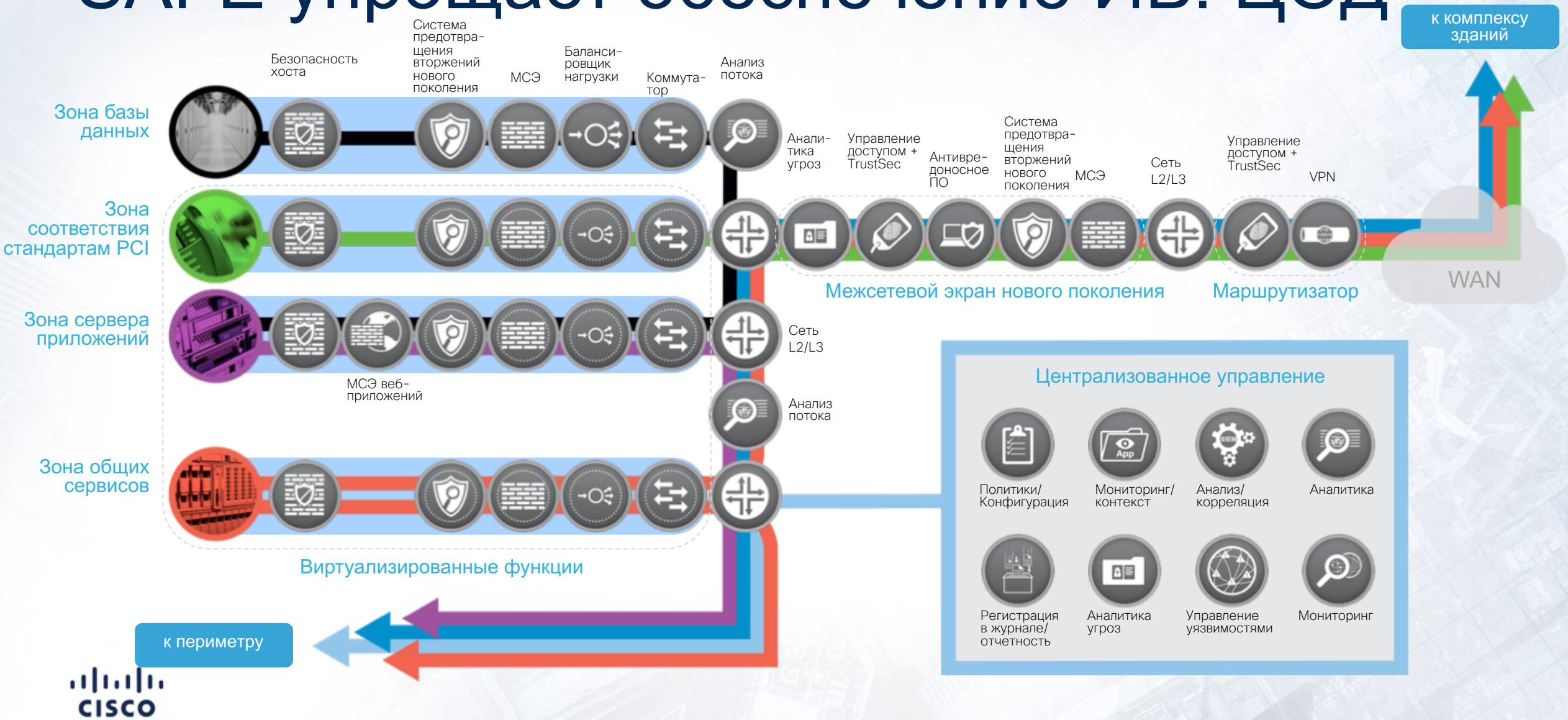


SAFE упрощает обеспечение ИБ: филиал

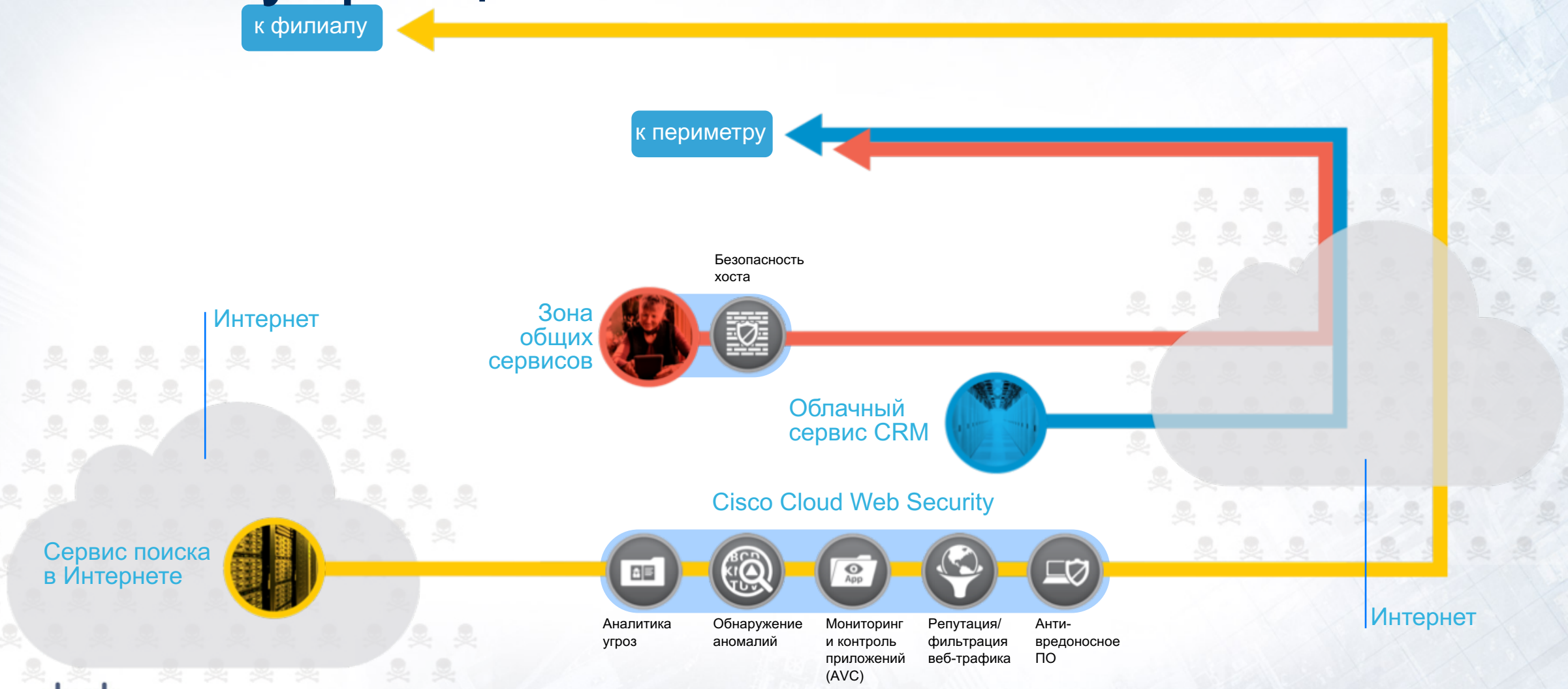


SAFE упрощает обеспечение ИБ: комплекс зданий

SAFE упрощает обеспечение ИБ: ЦОД



SAFE упрощает обеспечение ИБ: облако



SAFE упрощает обеспечение ИБ: внешние зоны

SAFE для вымогателей

Моделирование возможностей

- Думайте как хакер и попробуйте взломать себя
- Думайте как аудитор и попробуйте пройти аудит

Это не страшно!

cisco

Описание возможностей

- Маппируйте риски, угрозы и требования
- Найдите и нейтрализуйте все пробелы
- Оцените каждую возможность; если вы не можете ее реализовать - уберите

Угроза	Актуальная угроза	Требование	Возможность
Вредоносное ПО	Да	Да	AntiAPT / BDS / AV / NBAD
Утечки данных	Да	Нет	DLP / СКЗИ
DDoS	Нет	Нет	Anti-DDoS
Превышение привилегий	Да	Да	Разграничение доступа
НДВ	Нет	Нет	SAST/DAST
	Нет	Нет	
…			

Создание архитектуры безопасности

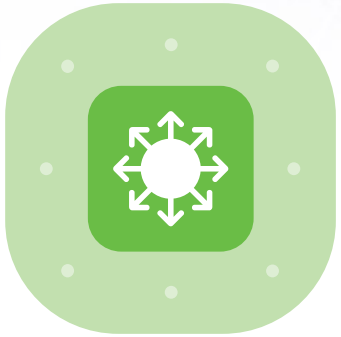
- Создание традиционного представления архитектуры
- Сопоставление возможностей с архитектурой
- Создание архитектуры, которая будет лучше всего отражать идентифицированные угрозы

Примерные компоненты архитектуры

МСЭ

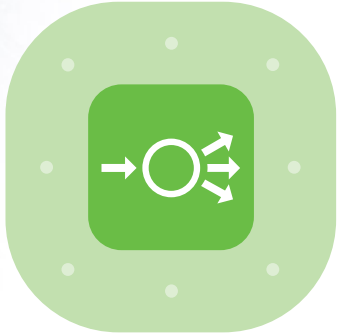
Маршрутизатор

Контроллер беспроводной сети



Коммутатор L3

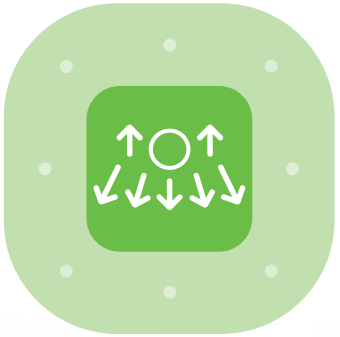
Обнаружение вторжений



Балансировщик нагрузки

Защищенный сервер

Хранение



Nexus 1Kv

Защита электронной почты

Компоненты архитектуры и возможности

- Какие возможности нужны?
- Какие компоненты архитектуры их могут реализовать?

МСЭ

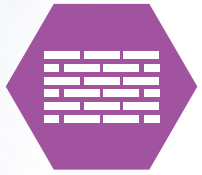
Коммутатор L3

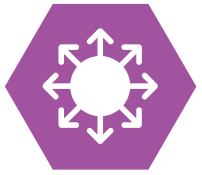
Стратегия архитектуры

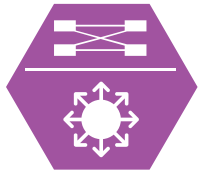
Создание дизайнов для обеспечения безопасности

- Создание традиционного представления дизайна
- Выбор продуктов, содержащих функциональные возможности, определенные в архитектуре
- Создание дизайна, наиболее подходящего для отражения ранее определенных угроз, и учитывающего дополнительные потребности инфраструктуры, например, высокую доступность, производительность и затраты

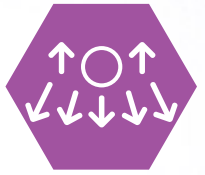
Примеры компонентов дизайна


МСЭ

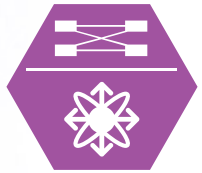

Коммутатор L3

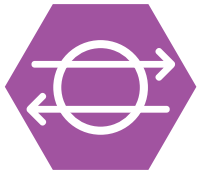

Коммутатор Catalyst для ЦОД

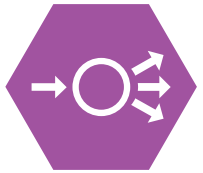
FirePOWER Устройство


Nexus 1Kv

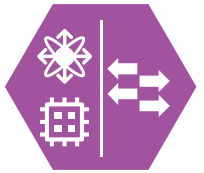

Защита электронной почты


Коммутатор Nexus для ЦОД


Обнаружение вторжений


Балансировщик нагрузки


Блейд-сервер


Коммутатор Nexus для фабрики


Коммутатор Nexus

Стратегия дизайна

Недоверенные

Проникновение наружу

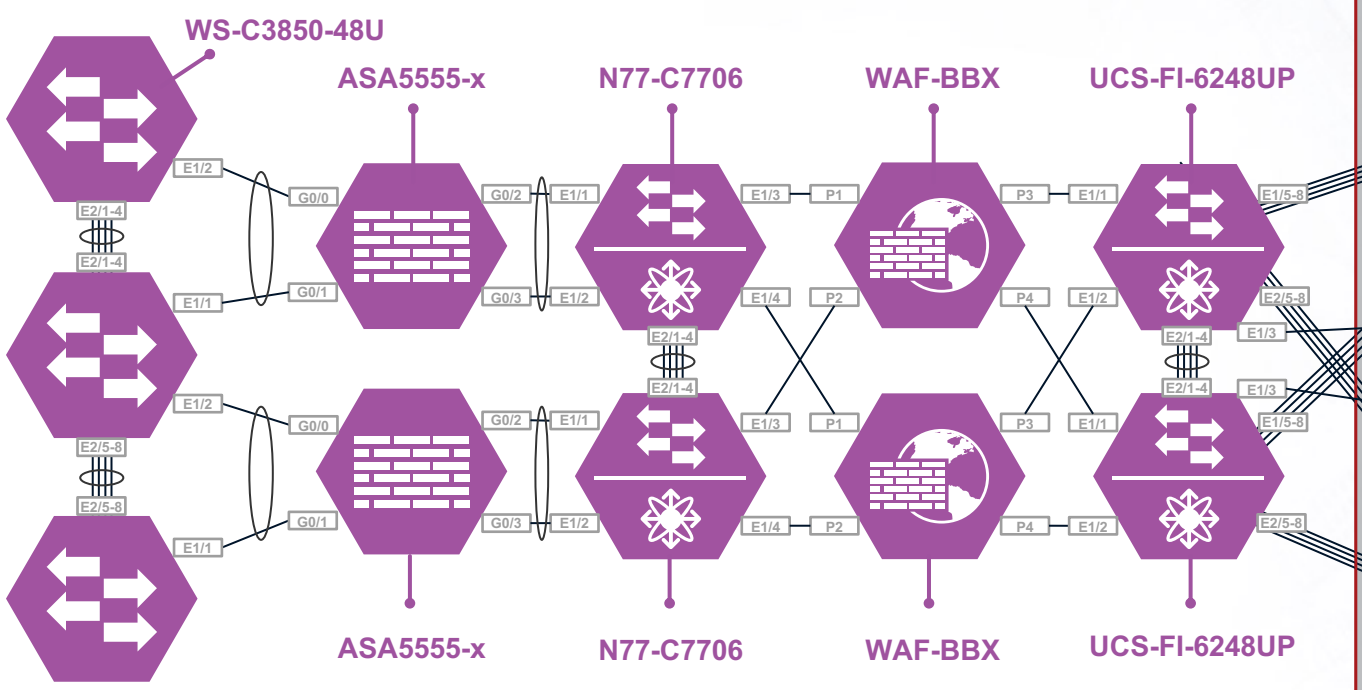
Черви

Трояны

Шпионское ПО

Угрозы

Место в сети



Политики/ конфигурация

Анализ/ корреляция

Мониторинг и контроль приложений (AVC)

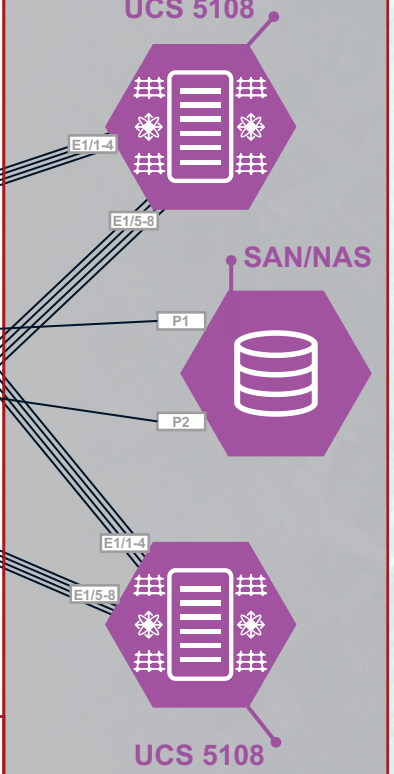
Регистрация в журнале/ отчетность

Мониторинг

Управление уязвимостями

Совместно используемые

Доверенные



Сервисы

А вдруг еще появятся требования? Кто их может установить?

Может ли быть что-то еще впереди?

Регуляторы

могут выпустить еще множество различных требований по защите информации, но они вряд ли добавят что-то новое к уже имеющемуся перечню, исключая специфичные отраслевые требования (и то не факт)

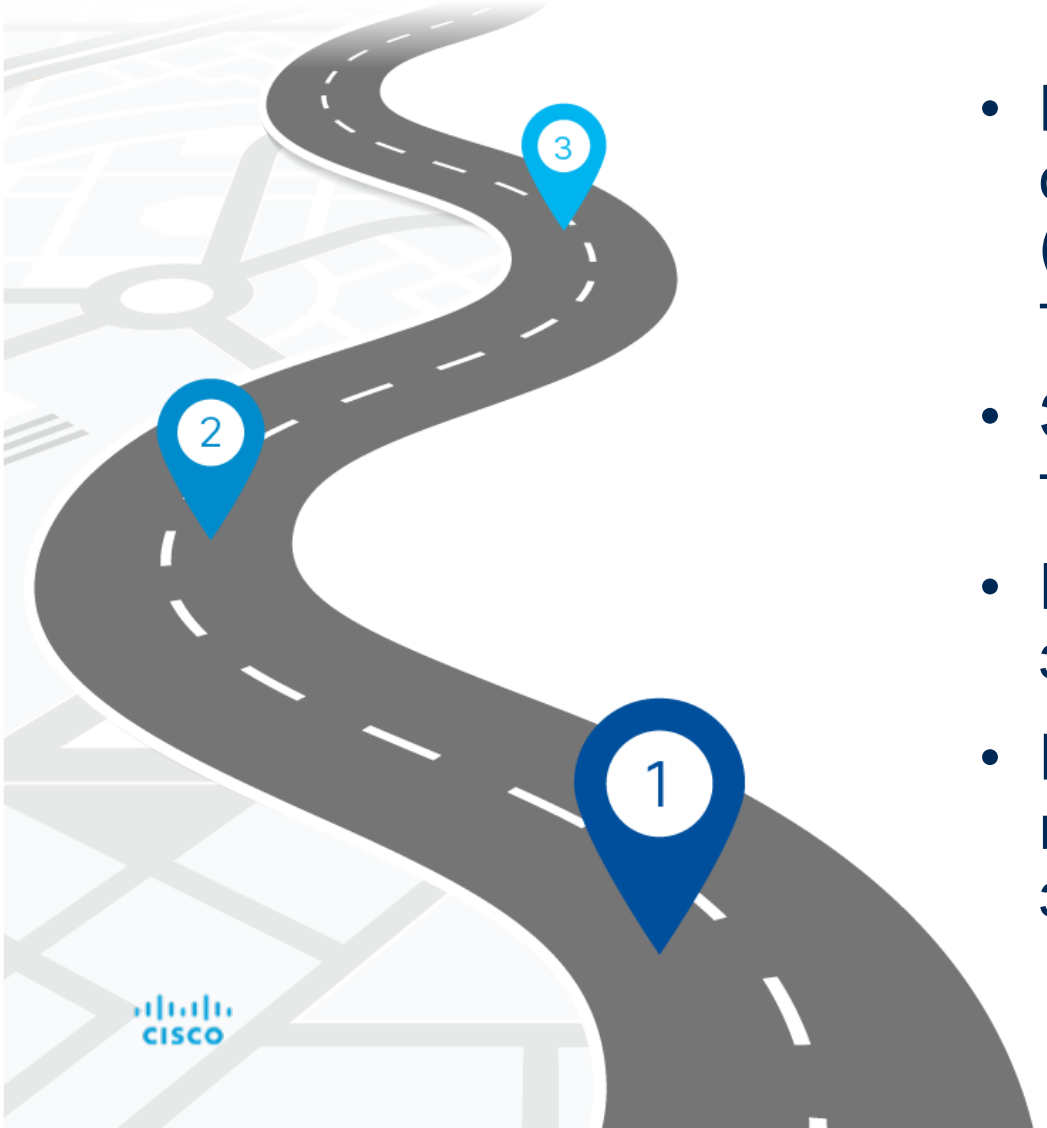
Основные регуляторы - ФСТЭК, ФСБ, Банк России

Еще регуляторы – МинЭнерго, Минкомсвязь

cisco

Давайте подводить черту

В качестве резюме



- В мире и даже в одной стране появляется огромное количество различных документов (от законов до best practices), которые требуют реализовывать защитные меры
- Защитных мер описано несколько сотен или тысяч
- Но базовых защитных мер, позволяющих закрыть до 85-95% атак, всего 2-3 десятка
- Начинайте с базовых защитных мер, постепенно расширяя их спектр в зависимости от модели угроз и нарушителя

Где вы можете узнать больше?

Пишите на security-request@cisco.com

Быть в курсе всех последних новостей вам помогут:

- http://www.facebook.com/CiscoRu
- http://twitter.com/CiscoRussia
- http://www.youtube.com/CiscoRussiaMedia
- http://www.flickr.com/photos/CiscoRussia
- http://vkontakte.ru/Cisco
- http://blogs.cisco.ru/
- http://habrahabr.ru/company/cisco
- http://linkedin.com/groups/Cisco-Russia-3798428
- http://slideshare.net/CiscoRu
- https://plus.google.com/106603907471961036146/posts
- http://www.cisco.ru/

Спасибо!

alukatsk@cisco.com