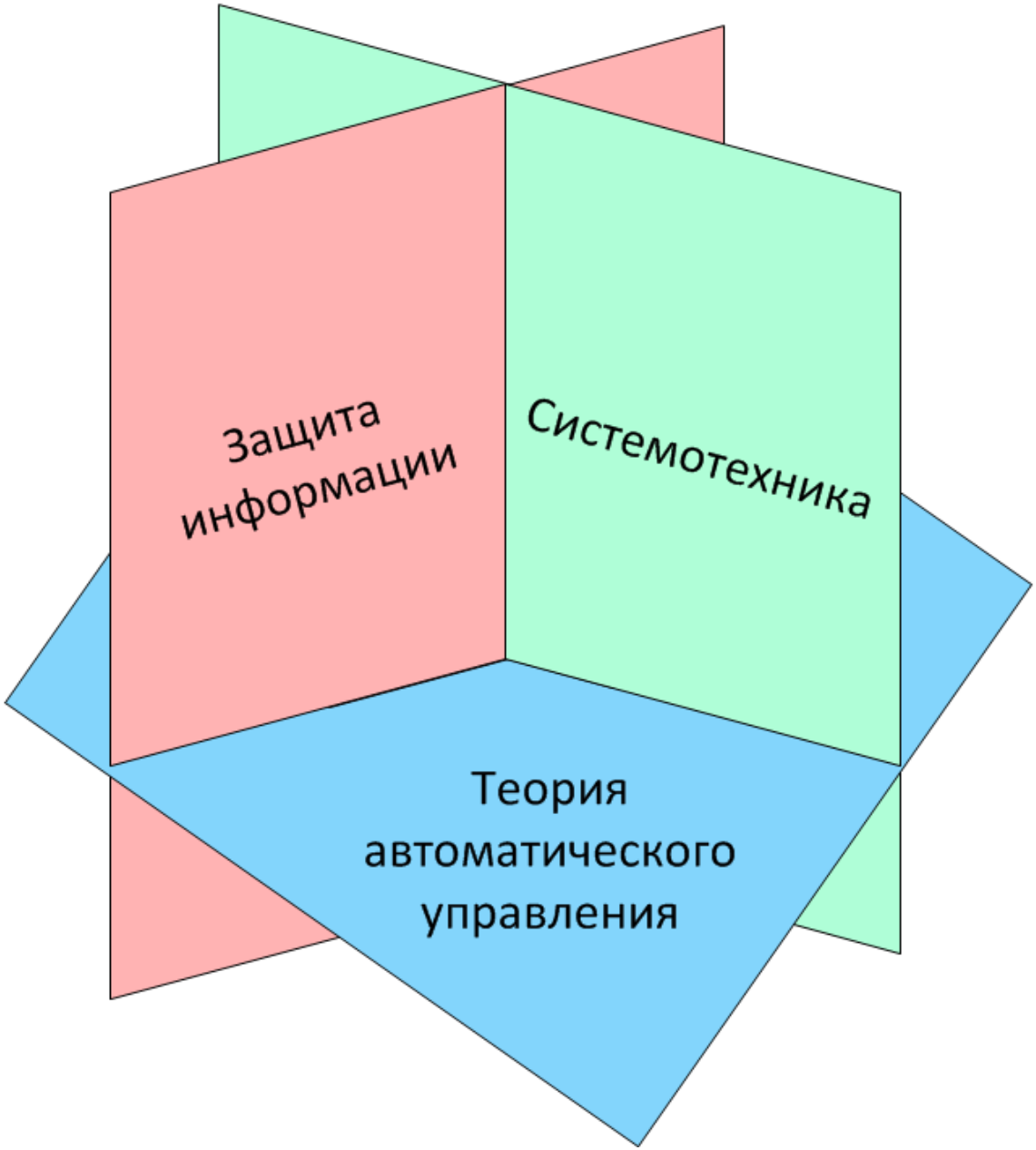
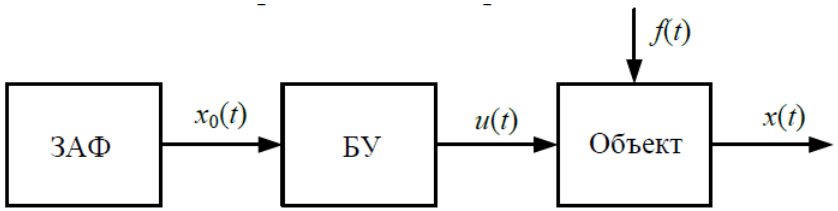
Безопасность АСУ ТП в 3D или головокружение без успехов

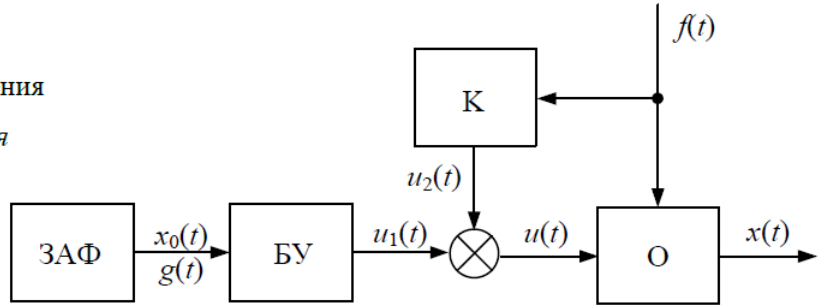


Фундаментальные принципы управления



ЗАФ – задатчик алгоритма функционирования; БУ – блок управления

Рис. 1.10. Функциональная схема разомкнутого управления



О – объект; К – компенсирующее устройство

Рис. 1.12. Функциональная схема системы управления по возмущению

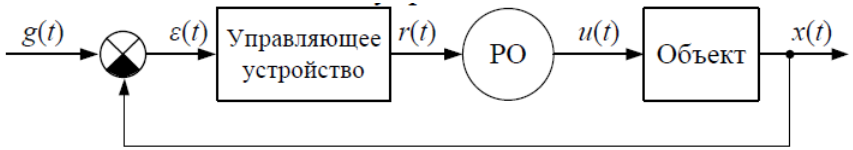


Рис. 1.14. Функциональная схема системы управления по отклонению

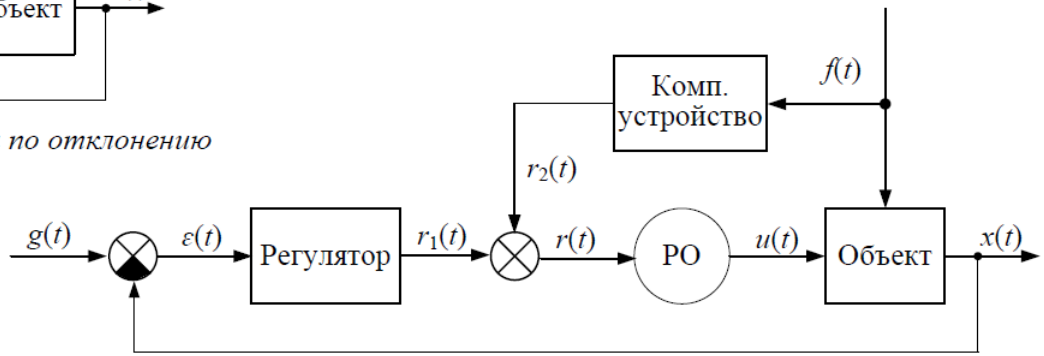


Рис. 1.16. Функциональная схема комбинированной САУ

Устойчивость объектов управления

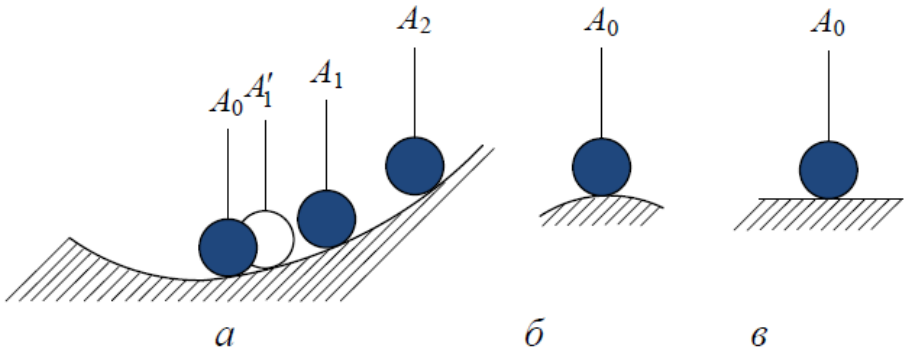
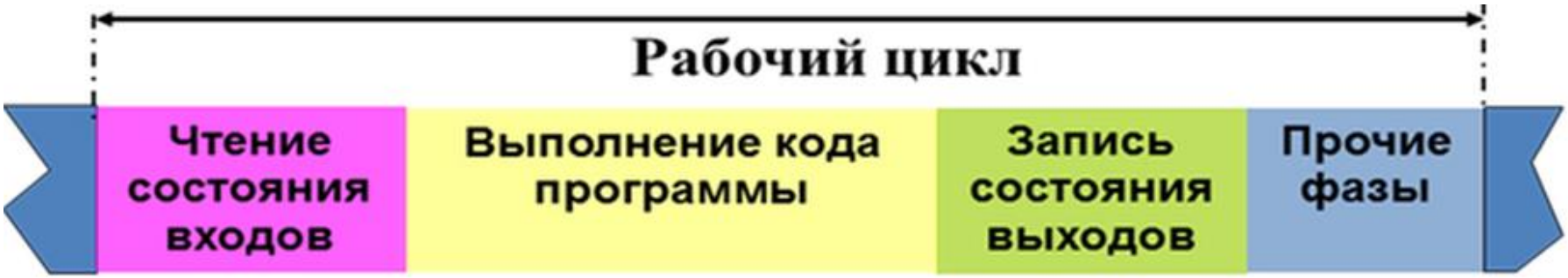
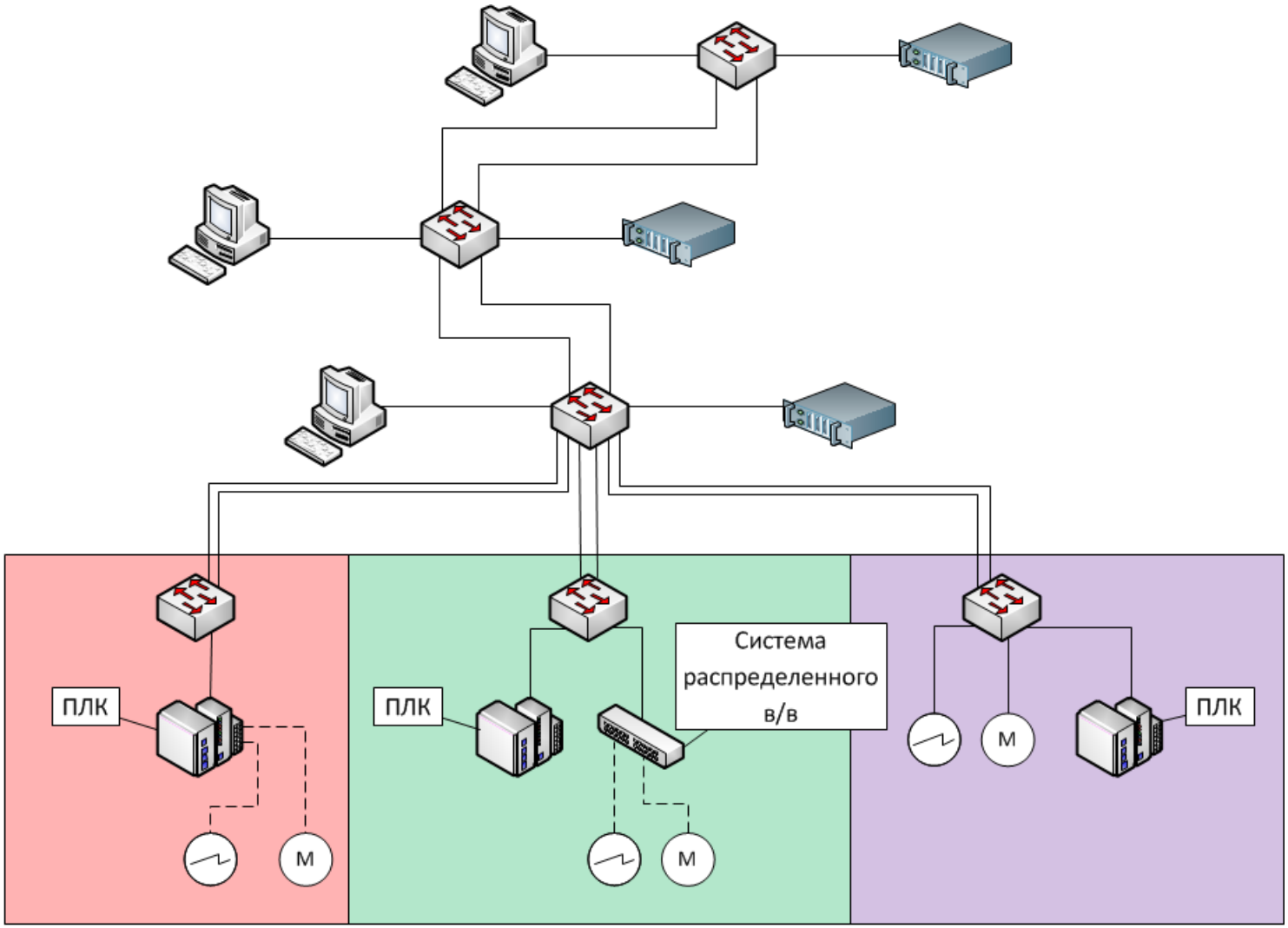


Рис. 4.1. Иллюстрация устойчивости положения равновесия системы: а – устойчивое; б – неустойчивое; в – безразличное

Циклы системы управления



Ландшафт систем управление в ближайшей окрестности настоящего



Устойчивость,
качество управления,
надежность

Пример творчества

Пример ответственного подхода

NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

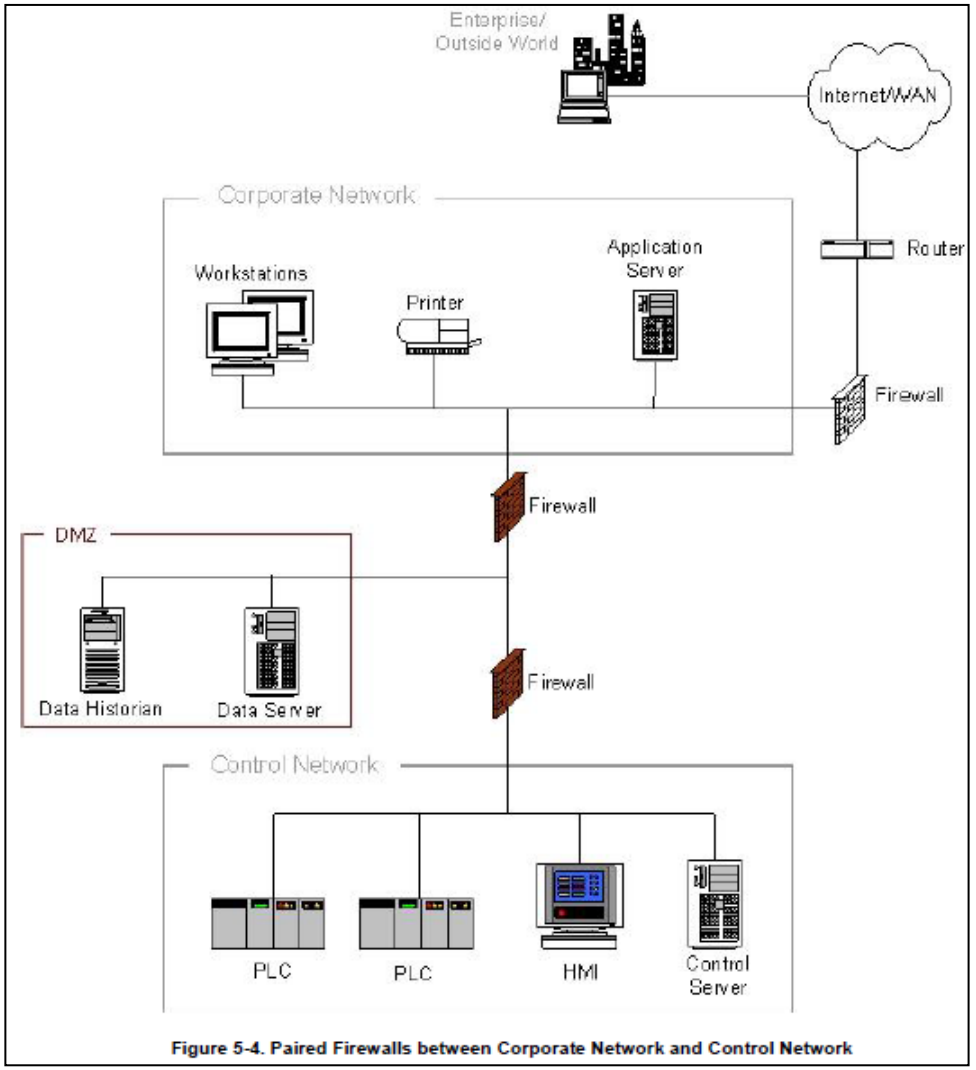
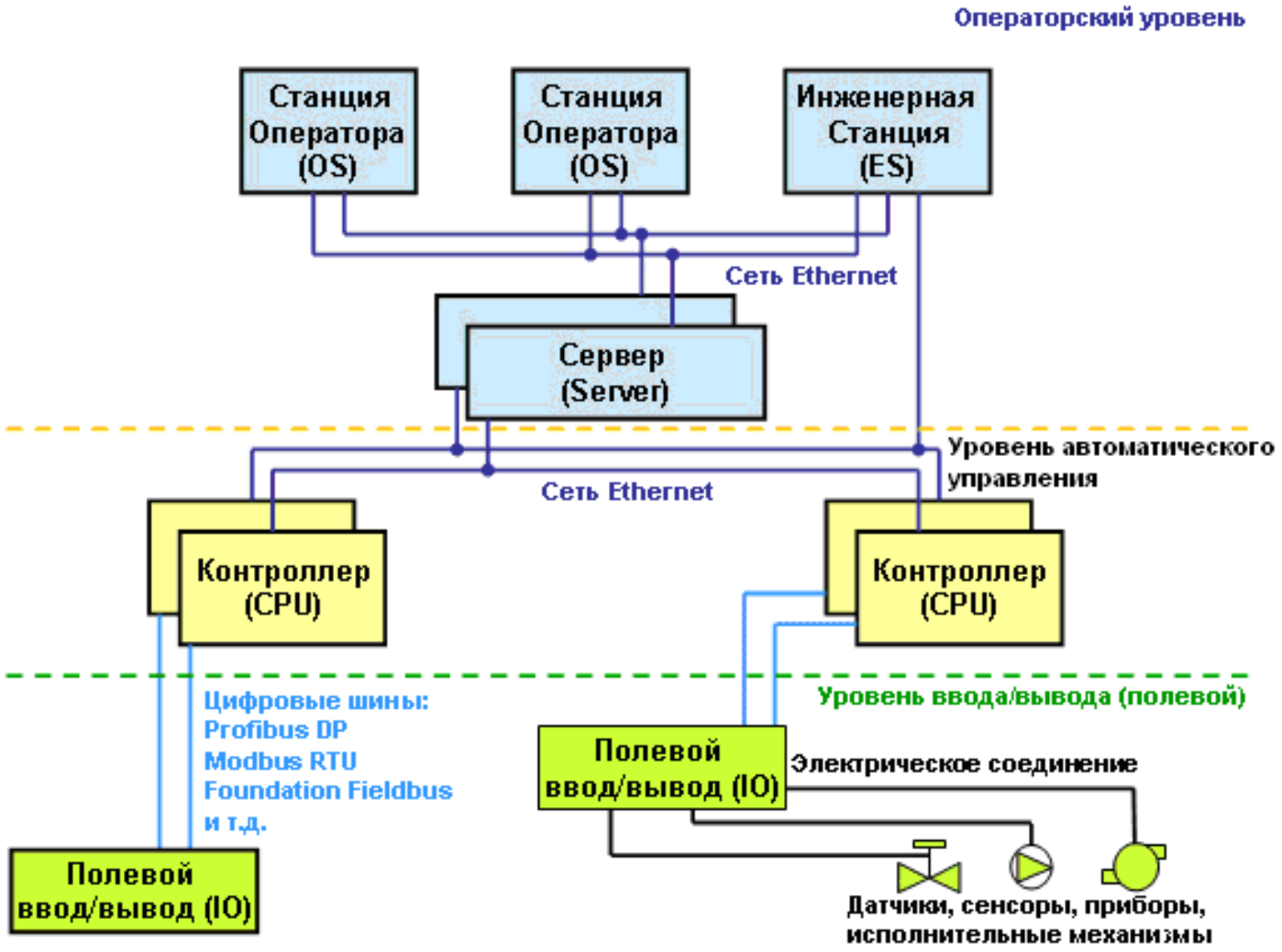


Figure 5-4. Paired Firewalls between Corporate Network and Control Network

Консерватория, аспирантура, … (© Михаил Жванецкий)



Может, что-то в консерватории подправить? (© Михаил Жванецкий)

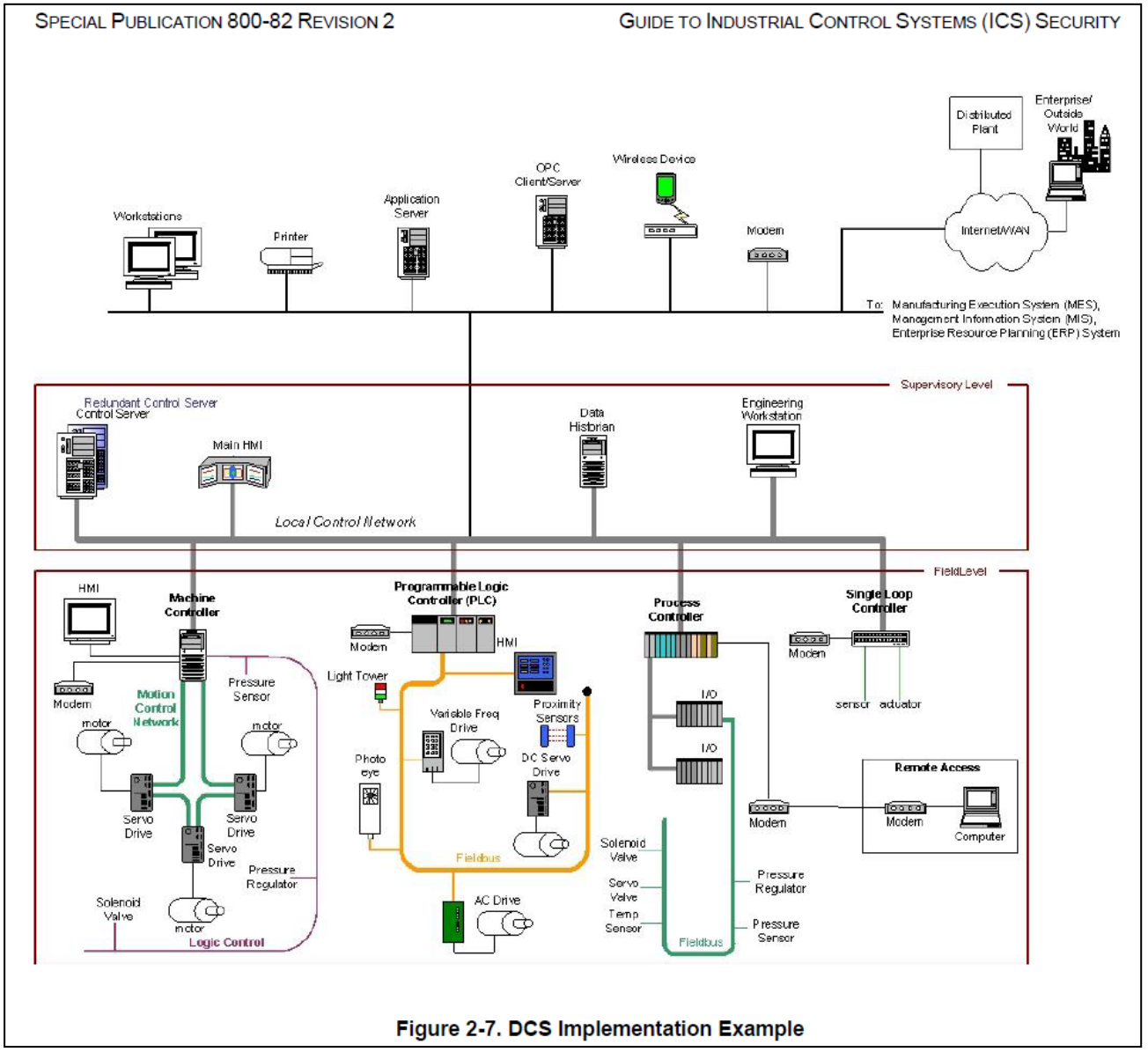
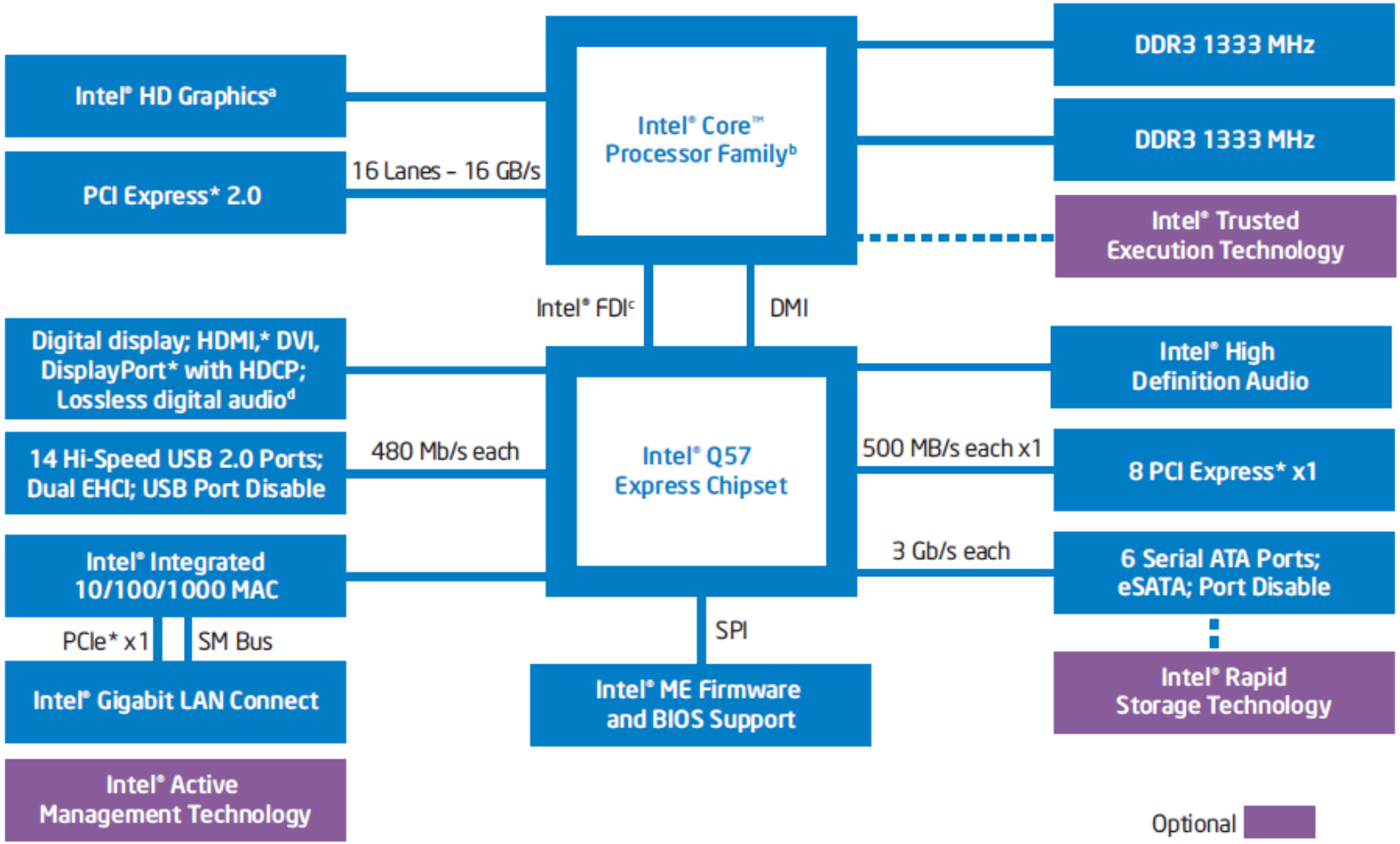


Figure 2-7. DCS Implementation Example

Этот железный зыбкий мир



Недостающее звено

У истоков

Не наш опыт

The Rainbow Series is six-foot tall stack of books on evaluating "Trusted Computer Systems" according to the National Security Agency. The term "Rainbow Series" comes from the fact that each book is a different color. The main book (upon which all other expound) is the Orange Book.

NSA/NCSC Rainbow Series – 27 книг.
Defense Department Rainbow Series – 10 книг.
Other NSA/NCSC Publications – порядка 18 книг.
Всего 56 книг.

Наш опыт

ФСТЭК России:

1. **Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.**
2. **Защита от несанкционированного доступа к информации. Термины и определения.**
3. **Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.**
4. **Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.**
5. **Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.**
6. **Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.**

Всего 6 книг.

Умудренные опытом

Не наш опыт

CSRC HOME > GROUPS > SMA > FISMA

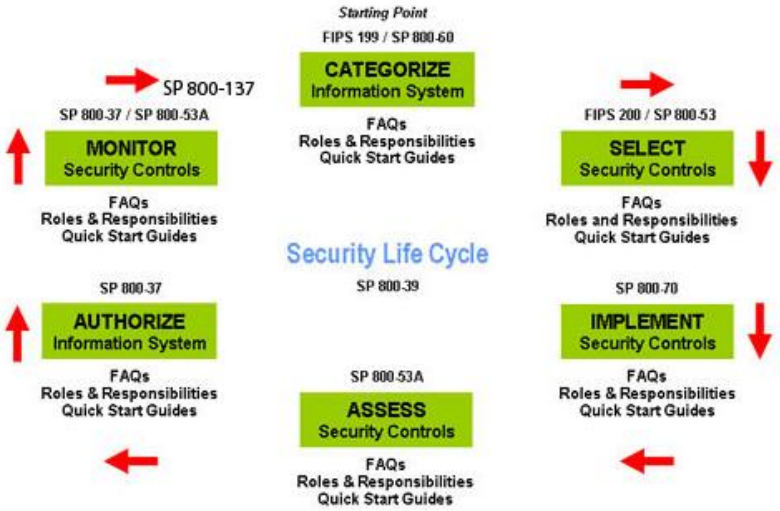
FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) IMPLEMENTATION PROJECT

Protecting the Nation's Critical Information Infrastructure

Our Vision

To promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act including:

Risk Management Framework



Наш опыт

Данный период характеризуется многовекторностью в стиле лебедя, рака и щуки. Единый замысел не просматривается.

Умудренные опытом

Не наш опыт

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

DEVELOPMENT SCHEDULE FOR FISMA IMPLEMENTATION PROJECT PUBLICATIONS

As of May 4, 2015

		Mar 2015	Apr 2015	May 2015	Jun 2015	Jul 2015	Aug 2015	Sep 2015	Oct 2015	Nov 2015	Dec 2015	Jan 2016	Feb 2016
FIPS 199	Final												
FIPS 200	Final												
SP 800-18, Rev 2 *Delayed*		RVC	RVC	RVC	RVC	RVC	RVC	RVC	RVC	IPD	RVC	RVC	Final
SP 800-30, Rev 1 *JTF*	Final												
SP 800-37, Rev 1 *JTF*	Final												
SP 800-39 *JTF*	Final												
SP 800-53, Rev 4 *JTF Errata Update*	Final												
SP 800-53A, Rev 4 *JTF Errata Update*	Final												
SP 800-59	Final												
SP 800-60, Rev 1	Final												
SP 800-60, Rev 2 *Delayed*		RVC	RVC	RVC	RVC	RVC	RVC	IPD	RVC	RVC	Final		
SP 800-137	Final												
SP 800-160 *Delayed*		RVC	RVC	RVC	RVC	RVC	2PD	RVC	RVC	FPD	RVC	RVC	Final
Ongoing Authorization Guidance	Final												

LEGEND: **1PD:** Initial public draft; **FPD:** Final public draft; **DEV:** Development cycle; **RVC:** Revision cycle; **ER**: Errata Update; **JTF:** Joint Task Force Transformation Initiative

FIPS PUB 199: *Standards for Security Categorization of Federal Information and Information Systems*
FIPS PUB 200: *Minimum Security Requirements for Federal Information and Information Systems*
SP 800-18, Revision 2: *Guide for Developing Security Plans for Federal Information Systems and Organizations* [4]
SP 800-30, Revision 1: *Guide for Conducting Risk Assessments* [1] [2]
SP 800-37, Revision 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* [2]
SP 800-39: *Managing Information Security Risk: Organization, Mission, and Information Systems View* [2]
SP 800-53, Revision 4: *Recommended Security and Privacy Controls for Federal Information Systems and Organizations* [2]
SP 800-53A, Revision 4: *Guide for Assessing the Security and Privacy Controls in Federal Information Systems and Organizations* [2] [4]
SP 800-59: *Guideline for Identifying an Information System as a National Security System*
SP 800-60, Revision 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*
SP 800-60, Revision 2: *Guide for Mapping Types of Information and Information Systems to Security Categories* [3] [4]
SP 800-137: *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
SP 800-160: *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*

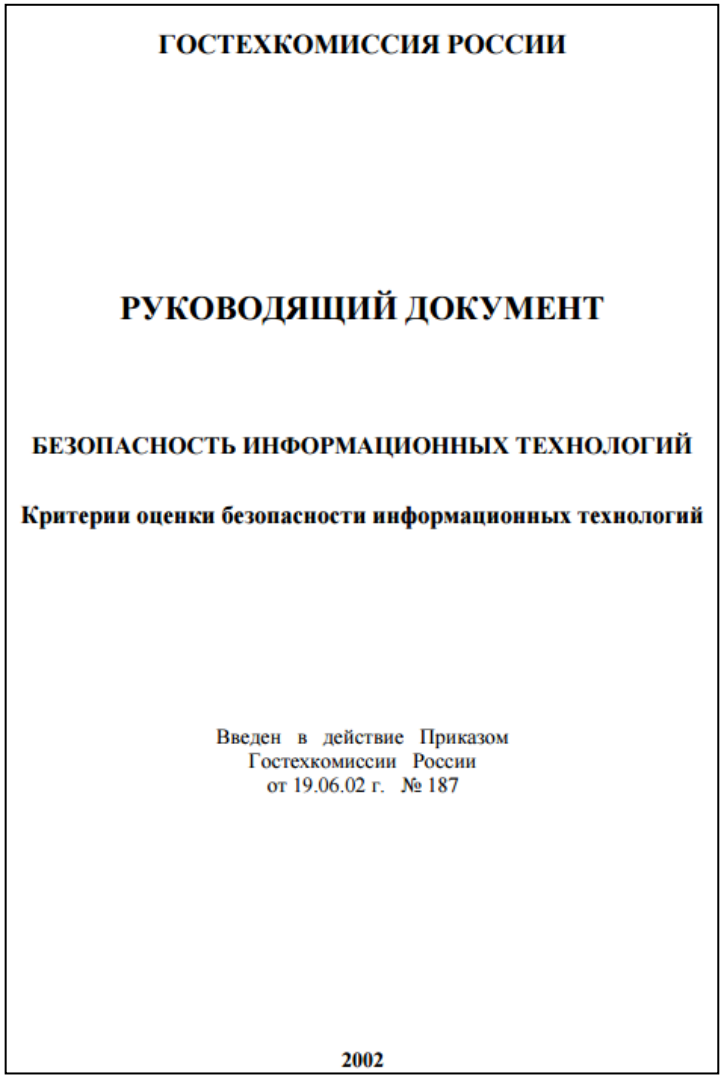
[1] Publication refocused to address only risk assessments.
[2] Publication developed as part of the Joint Task Force Transformation Initiative (DOD, ODNI, CNSS, and NIST).
[3] Publication being updated to be consistent with NARA Controlled Unclassified Information (CUI) types in response to Executive Order 13556.
[4] Publications delayed due to a change in organizational priorities.

Умудренные опытом

Наш опыт

ФСТЭК России

Планомерная деятельность по поддержанию жизненного цикла документов отсутствует.



ГОСТЕХКОМИССИЯ РОССИИ

РУКОВОДЯЩИЙ ДОКУМЕНТ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Критерии оценки безопасности информационных технологий

Введен в действие Приказом
Гостехкомиссии России
от 19.06.02 г. № 187

2002

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-1— 2012

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.
КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

Введение и общая модель

ISO/IEC 15408-1:2009
Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

(IDT)

Издание официальное

Москва
Стандартинформ
2014

Умудренные опытом

Не наш опыт

NIST, ISO/IEC, и другие:

FIPS – порядка 18 книг.

SP – порядка 177 книг.

Common Criteria for Information Technology Security Evaluation – 3 книги.

Common Methodology for Information Technology Security Evaluation – 1 книга.

15408 – 3 книги.

15446 – 1 книга.

19791 – 1 книга.

Наш опыт

ФСТЭК России и Федеральное агентство по техническому регулированию и метрологии:

Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (ну очень старый 15408) – 3 книги.

Половинка четырехтомника по защите ПДн от 2008 года – 2 книги.

Документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (ДСП) – 7 книг.

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (приказ №17) – 1 книга.

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ №21) – 1 книга.

Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (приказ №31) – 1 книга.

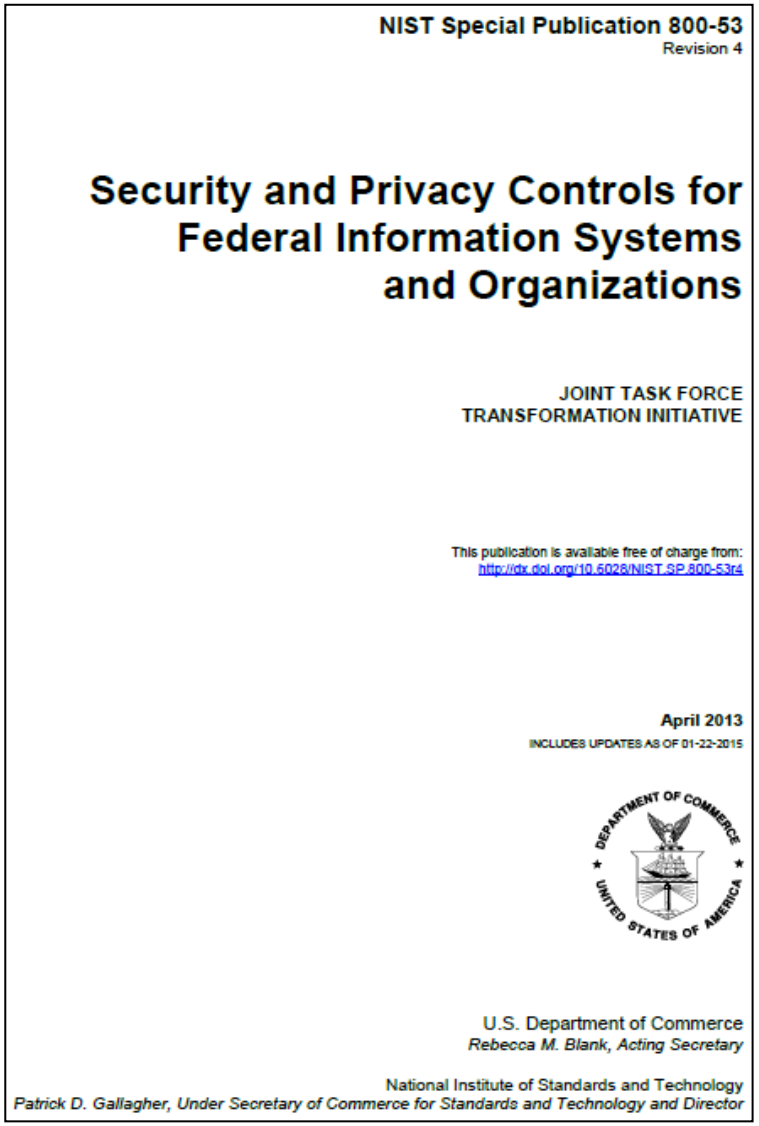
15408 – 3 книги.

15446 – 1 книга.

19791 – 1 книга.

Умудренные опытом

Не наш опыт



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

April 2013
INCLUDES UPDATES AS OF 01-22-2015

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Наш опыт

ФСТЭК России:

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (приказ №17) – 1 книга.

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ №21) – 1 книга.

Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (приказ №31) – 1 книга.

Фактически все три документа содержат некую преамбулу за которой следует творчески урезанная версия «APPENDIX D SECURITY CONTROL BASELINES – SUMMARY» из SP 800-53. При этом полностью опущен «APPENDIX F SECURITY CONTROL CATALOG» который очень полезен для понимания APPENDIX D.

Умудренные опытом

Не наш опыт

IA-9	Service Identification and Authentication
IA-9(1)	*SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*
IA-9(2)	*SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

Control: The organization identifies and authenticates [*Assignment: organization-defined information system services*] using [*Assignment: organization-defined security safeguards*].

Supplemental Guidance: This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.

Control Enhancements:

(1) *SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*

The organization ensures that service providers receive, validate, and transmit identification and authentication information.

(2) *SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*

The organization ensures that identification and authentication decisions are transmitted between [*Assignment: organization-defined services*] consistent with organizational policies.

Supplemental Guidance: For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification and authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification and authentication decisions (as opposed to the actual identifiers and authenticators) to the services that need to act on those decisions. Related control: SC-8.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

Наш опыт

Приказ №31:

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

Умудренные опытом

Наш опыт

Приказ №31:

/*

Степень возможного ущерба:

- высокая, если в результате нарушения одного из свойств безопасности информации возможно возникновение чрезвычайной ситуации федерального или межрегионального характера или иные существенные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;
- средней, если в результате нарушения одного из свойств безопасности информации возможно возникновение чрезвычайной ситуации регионального или межмуниципального характера или иные умеренные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;
- низкой, если в результате нарушения одного из свойств безопасности информации возможно возникновение чрезвычайной ситуации муниципального (локального) характера или возможны иные незначительные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности.

*/

Шкала градаций не рабочая!!!

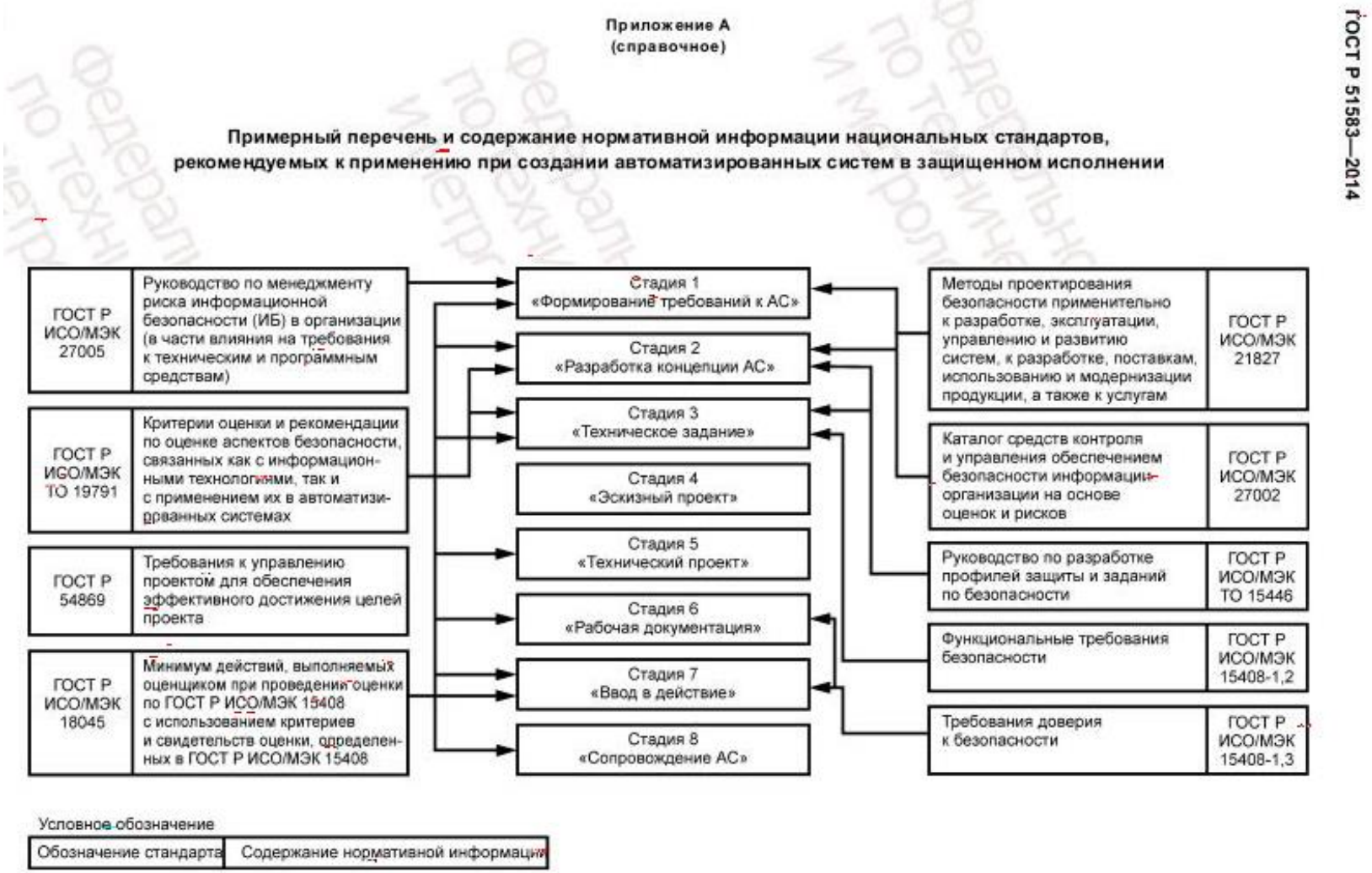
Если реализована противоаварийная защита (ПАЗ), то вероятность возникновения чрезвычайной ситуации практически стремиться к нулю.

Если брать экономическую или социальную составляющую, то степень ущерба всегда будет стремиться к высокому значению.

Умудренные опытом

Наш опыт

ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».



Приложение А
(справочное)

ГОСТ Р 51583—2014

Примерный перечень и содержание нормативной информации национальных стандартов, рекомендуемых к применению при создании автоматизированных систем в защищенном исполнении

ГОСТ Р ИСО/МЭК 27005	Руководство по менеджменту риска информационной безопасности (ИБ) в организации (в части влияния на требования к техническим и программным средствам)	Стадия 1 «Формирование требований к АС»	Стадия 2 «Разработка концепции АС»	Методы проектирования безопасности применительно к разработке, эксплуатации, управлению и развитию систем, к разработке, поставкам, использованию и модернизации продукции, а также к услугам	ГОСТ Р ИСО/МЭК 21827
ГОСТ Р ИСО/МЭК ТО 19791	Критерии оценки и рекомендации по оценке аспектов безопасности, связанных как с информационными технологиями, так и с применением их в автоматизированных системах	Стадия 3 «Техническое задание»	Стадия 4 «Эскизный проект»	Каталог средств контроля и управления обеспечением безопасности информации организации на основе оценок и рисков	ГОСТ Р ИСО/МЭК 27002
ГОСТ Р 54869	Требования к управлению проектом для обеспечения эффективного достижения целей проекта	Стадия 5 «Технический проект»	Стадия 6 «Рабочая документация»	Руководство по разработке профилей защиты и заданий по безопасности	ГОСТ Р ИСО/МЭК ТО 15446
ГОСТ Р ИСО/МЭК 18045	Минимум действий, выполняемых оценщиком при проведении оценки по ГОСТ Р ИСО/МЭК 15408 с использованием критериев и свидетельств оценки, определенных в ГОСТ Р ИСО/МЭК 15408	Стадия 7 «Ввод в действие»	Стадия 8 «Сопровождение АС»	Функциональные требования безопасности	ГОСТ Р ИСО/МЭК 15408-1,2
				Требования доверия к безопасности	ГОСТ Р ИСО/МЭК 15408-1,3

Условное обозначение

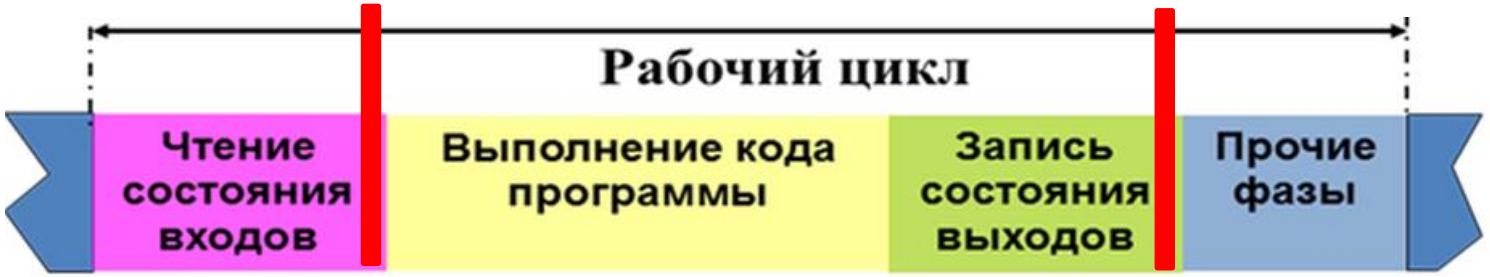
Обозначение стандарта	Содержание нормативной информации

Что делать то?

«Победоносная армия сначала осознает условия победы, а затем ищет битвы; проигравшая армия сначала сражается, а затем ищет победу» (Сунь Цзы)

Условия победы

1. Научиться видеть и правильно интерпретировать увиденное.
2. Готовность к кооперации.
3. Решение вопросов безопасности на этапе разработки системы управления.
4. Встраивание в компоненты системы управления и интегрированную среду разработки функций безопасности реального времени.



Все зависит от нас

nav7ad@mail.ru, Неклюдов Андрей