# Российское и зарубежное законодательство в области ИБ. Обзор международных и национальных стандартов и спецификаций в области ИБ: «Оранжевая книга», ИСО 15408

Программное обеспечение в нашей стране регламентировано основополагающим стандартом ГОСТ Р 51904-2002 «Программное обеспечение встроенных систем. Общие требования к разработке и документированию», который утвержден и введен в действие постановлением Госстандарта России от 25.06.2002 № 247. Данный стандарт подготовлен в развитие ГОСТ Р ИСО/МЭК 12207-99 «Информационные технологии. Процессы жизненного цикла программных средств».

Стандарт ГОСТ Р 51904-2002 предусматривает все необходимые требования к разработке ПО, а также требования к составу и оформлению разрабатываемой документации и тестированию ПО. Помимо упомянутых выше, стандарт содержит в своем составе следующие разделы, каждый из которых подробно развернут:

1) «Общие требования»;
2) «Системные аспекты, связанные с разработкой ПО»;
3) «Процесс планирования ПО»;
4) «Процессы разработки ПО»;
5) «Процесс верификации ПО»;
6) « Процесс управления конфигурацией ПО»;
7) «Процесс обеспечения качества ПО»;
8) «Процесс сертификационного сопровождения»;
9) «Документы, создаваемые в процессах жизненного цикла ПО».

# ПО делится

*Системные* программы управляют взаимодействием компонентов самого компьютера, а *прикладные* программы предназначены для решения внешних задач, например обработки текстов или воспроизведения видеоинформации. В этом случае выдается сертификат на ПО в соответствии с ГОСТ 19781-90.

*Базовое* программное обеспечение, в свою очередь, включает в себя:

- операционные системы (OS/2, Windows NT/ XP, Unix, Solaris);
- операционные оболочки:
- сетевые операционные системы (обеспечивают обработку, передачу и хранение данных в Интернете);
- систему управления файлами;
- системные утилиты.

Современное состояние развития ПО показывает, что эти сегменты сливаются в глобальные операционные системы, выполняющие функции всех этих элементов.

*Сервисное* программное обеспечение (прикладные программы) можно классифицировать по функциональному признаку (ГОСТ Р ИСО/МЭК ТО 12182-2002) и разделить на следующие категории:

- программы диагностики работоспособности компьютера и обслуживания дисков (утилиты):
- архиваторы;
- антивирусные программы;
- текстовые редакторы;
- программы для работы с видео;
- программы для работы с аудио;
- программы шифрования;
- программы для работы с почтой;
- интернет-браузеры;
- программы для закачки файлов из Интернета (менеджеры закачки) и многие другие.

# Стандарты информационной безопасности

- это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам.

# Функции стандартов в области ИБ

- **- выработка понятийного аппарата и терминологии в области информационной безопасности**
- **- формирование шкалы измерений уровня информационной безопасности**
- **- согласованная оценка продуктов, обеспечивающих информационную безопасность**
- **- повышение технической и информационной совместимости продуктов, обеспечивающих ИБ**
- **- накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории – производителям средств ИБ, экспертам, ИТ-директорам, администраторам и пользователям информационных систем**
- **- функция нормотворчества – придание некоторым стандартам юридической силы и установление требования их обязательного выполнения.**

# Роль стандартов по ИБ

| производители и эксперты | потребители |
| --- | --- |
| • обоснованно определяют наборы требований к информационным продуктам и декларируют их возможности<br>• подтверждают ценность продуктов путем сертификации на соответствие стандартам ИБ<br>• получают ценную техническую и иную информацию | • обоснованно выбирают информационные продукты<br>• более четко формулируют требования к ним<br>• имеют возможность построить гарантированно качественную систему ИБ |

# Основными областями стандартизации информационной безопасности являются:

- аудит информационной безопасности
- модели информационной безопасности
- методы и механизмы обеспечения информационной безопасности
- криптография
- безопасность межсетевых взаимодействий
- управление информационной безопасностью.

# Специалист , имеющему отношение к информационной безопасности, должен знать:

- терминологию в сфере ИБ;
- общие подходы к построению ИБ;
- общепринятые процессы ИБ и рекомендации по их выстраиванию;
- конкретные меры защиты — контроли ИБ;
- роли и зоны ответственности при построении процессов ИБ;
- подходы к измерению зрелости процессов ИБ;
- и многое другое.

# Стандарты можно поделить на:

**Технические или контрольные (control)**

- **Технические стандарты помогают провести выстраивание технической защиты информации — выбрать необходимый комплекс защитных мер и провести их грамотную настройку**
- дают практические рекомендации и отвечают на вопрос **«как реализовать?»**
- серия ISO/IEC 27XXX, руководство ITIL, методология COBIT

**Процессно-ориентированные**

- **описывают поход к выстраиванию отдельных процессов**
- позволяют ответить на вопросы **«что делать?»**
- проект OWASP top 10, CIS Controls, CIS Benchmarks

# МЕЖДУНАРОДНЫЕ СТАНДАРТЫ В ОБЛАСТИ ИБ

# COBIT

- Основой стандарта являются 40 высокоуровневых целей контроля, сгруппированных в четыре домена, два из которых посвящены информационной безопасности):
- «COBIT 2019 Framework: Introduction and Methodology» — «COBIT 2019 Бизнес-модель: Введение и методология».
- «COBIT 2019 Framework: Governance and Management Objectives» — «COBIT 2019 Бизнес-модель: Задачи руководства и управления.
- «COBIT 2019 DESIGN GUIDE: Designing an Information and Technology Governance Solution — «Проектирование решения по руководству информацией и технологиями».
- «COBIT 2019 IMPLEMENTATION GUIDE: Implementing and Optimizing an Information and Technology Governance Solution» — «Внедрение и оптимизация решения по руководству информацией и технологиями».

# ITIL и ITSM

- Библиотека инфраструктуры информационных технологий или ITIL (The IT Infrastructure Library) — это набор публикаций (библиотека), описывающий общие принципы эффективного использования ИТ-сервисов. Библиотека ITIL применяется для практического внедрения подходов IT Service Management (ITSM) — проектирования сервисов и ИТ-инфраструктуры компании, а также обеспечения их связности.

# Серия ISO/IEC 27XXX

Самый известный стандарт серии — ISO/IEC 27001:2013, определяющий аспекты менеджмента информационной безопасности и содержащий лучшие практики по выстраиванию процессов для повышения эффективности управления ИБ.

Стандарт ISO/IEC 27001:2013 состоит из двух частей:

- Описание подхода к созданию СУИБ;
- Приложение А (требования ИБ и средства их реализации , структурированные по разделам).

# ISO/IEC 15408

- Еще одним стандартом, применяемым зарубежными ИБ-специалистами, является ISO 15408, состоящий из трех частей:
- ISO/IEC 15408-1:2009 Evaluation criteria for IT security — Part 1: Introduction and general model — «Общие критерии оценки безопасности информационных технологий».
- ISO/IEC 15408-2:2008 Evaluation criteria for IT security — Part 2: Security functional components model — «Функциональные компоненты безопасности».
- ISO/IEC 15408-3:2008 Evaluation criteria for IT security — Part 3: Security assurance components — «Компоненты доверия к безопасности».

# ISO/IEC 15408

- Первая часть стандарта содержит единые критерии оценки безопасности ИТ-систем на программно-аппаратном уровне, известна как «Оранжевая книга»
- Вторая часть приводит требования к функциональности средств защиты, которые могут быть использованы при анализе защищенности для оценки полноты реализованных функций безопасности.
- Третья часть серии содержит обоснования угроз, политик и требований. Стандарт определяет компоненты доверия к безопасности, каталогизирует наборы компонентов и классов доверия.

# NIST

- NIST — National Institute of Standards and Technology — американский национальный институт стандартизации, аналог отечественного Госстандарта. В состав института входит Центр по компьютерной безопасности, который публикует с начала 1990-х годов Стандарты (FIPS), а также детальные разъяснения/рекомендации (Special Publications) в области информационной безопасности.

# SANS. CIS 20

- SANS — организация по обучению и сертификации в области ИБ, наиболее известна своими руководствами по безопасной настройке различных систем (Benchmarks) и перечнем ключевых мер защиты Top 20 Critical Security Controls (CSC), включающим 20 рекомендаций по защите ИТ-инфраструктуры.
- ИБ-специалисты могут использовать этот документ как контрольный список при проверке безопасности систем.

# SANS. CIS 20

- Руководства CIS Benchmarks — очень полезный инструмент при настройке или проверке различных элементов ИТ-инфраструктуры на предмет защищенности. Полный перечень включает около 140 наставлений, сгруппированных по разным темам: .
- Desktops & Web Browsers
- Mobile Devices
- Network Devices
- Security Metrics
- Servers – Operating Systems
- Servers – Other
- Virtualization Platforms & Cloud