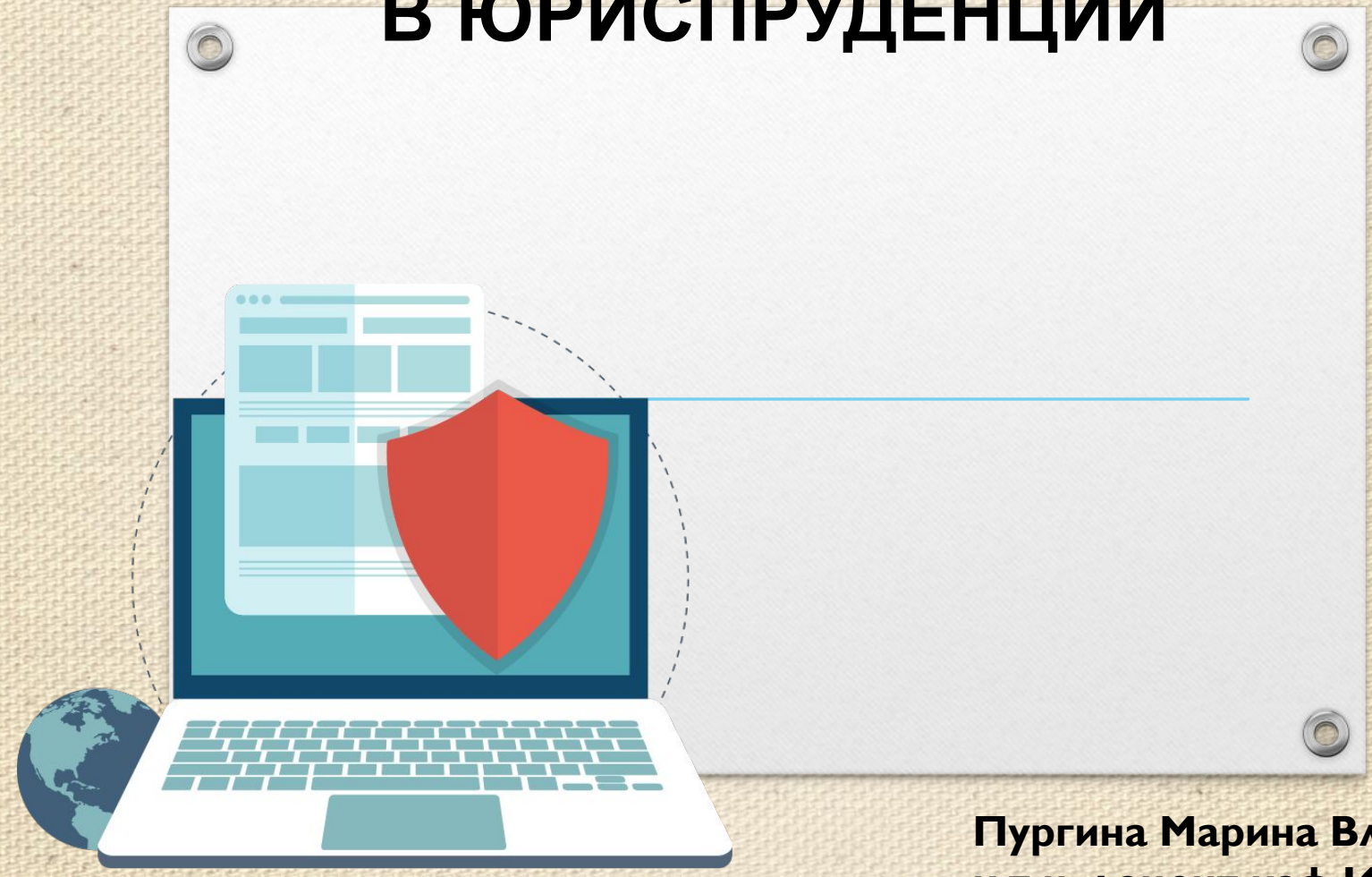
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИСПРУДЕНЦИИ



Пургина Марина Владимировна
к.т.н, доцент каф.ИТ
pur-11@yandex.ru

Стандарты и спецификации в области информационной безопасности

Понятие стандарта

ФЗ«О техническом регулировании»
№184-ФЗ 2002 г. (в ред. ФЗ № 45-ФЗ 2005 г.)

СТАНДАРТ **-** документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг.

СТАНДАРТИЗАЦИЯ **-** деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

ФЗ«О техническом регулировании» №184-ФЗ 2002 г. (в ред. ФЗ № 45-ФЗ 2005 г.)

Основные цели реформирования системы технического регулирования:

1. снижение административного и экономического давления на производителей;
2. расширение возможностей производителей за счет устранения соблюдаемых ранее ими избыточных требований и процедур;
3. устранение технических барьеров в торговле;
4. повышение эффективности защиты рынка от опасной продукции.

Знания стандартов и спецификаций

Обязательность следования стандартам и спецификациям в ряде случаев закреплена законодательно.

В стандартах и спецификациях зафиксированы апробированные, высококачественные решения и методологии.

Стандарты и спецификации являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов.

Для кого необходимо знание стандартов и спецификаций

- Разработчикам средств защиты и защищенных ИС;
- Системным и сетевым администраторам;
- Администраторам безопасности;
- Руководителям соответствующих служб и пользователям.

ФЗ«О техническом регулировании»
№184-ФЗ 2002 г. (в ред. ФЗ № 45-ФЗ 2005 г.)

Роль стандарта:

- формирование доказательной базы;
- соблюдения технических регламентов;
- повышение конкурентоспособности продукции, работ и услуг.

Начиная с начала 80-х годов XXв. были созданы десятки *международных стандартов* в области информационной безопасности, дополняющих друг друга, например:

- Критерий оценки надежности компьютерных систем «Оранжевая книга» (США);
- Рекомендации X.800;
- Германский стандарт BSI;
- Британский стандарт BS 7799;
- Стандарт ISO 17799;
- Стандарт «Общие критерии» ISO 15408;
- Стандарт COBIT.

ОСНОВНЫЕ ГРУППЫ СТАНДАРТИЗИРУЮЩИХ ДОКУМЕНТОВ В ОБЛАСТИ ИБ

Все эти стандарты можно разделить на два вида:

- ОЦЕНОЧНЫЕ СТАНДАРТЫ - предназначены для оценки и классификации информационных систем и средств защиты по требованиям безопасности;

- ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ (регламенты) - регламентируют различные аспекты реализации и использования средств и методов защиты.

В Оранжевой книге:

- Заложен *понятийный базис ИБ*: безопасная и доверенная системы, политика безопасности, уровень гарантированности, подотчетность, ядро и периметр безопасности и т.д.

- Описаны *основные механизмы формализации политики безопасности*: дискреционное и мандатное управление доступом, безопасность повторного использования объектов, метки безопасности.

- Сформулированы *принципы классификации по требованиям безопасности* на основе шкалы уровней доверия (D, C, B, A) и классов безопасности (C1, C2, B1, B2, B3, A1).

- *Повышение защищенности* обеспечивается параллельным усилением требований к политике безопасности и уровню гарантированности.

Механизмы безопасности Оранжевой книги

Политика безопасности должна включать следующие элементы:

1. Произвольное управление доступом – метод разграничения доступа к объектам, основанный на учете личности субъекта;
2. Безопасность повторного использования объектов – средство управления доступом, предохраняющее от случайного или преднамеренного извлечения информации из областей оперативной или дисковой памяти;
3. Метки безопасности – специальные идентификаторы определяющие уровни секретности объектов и субъектов;
4. Принудительное управление доступом – управление доступом к объектам основанное на сопоставлении меток безопасности субъектов и объектов.

Рекомендации X.800.
Сетевые сервисы безопасности

Функции (сервисы) безопасности включают:

- аутентификацию;
- управление доступом;
- конфиденциальность данных;
- целостность данных;
- неотказуемость.

Германский стандарт BSI

В 1998 году в Германии вышло "Руководство по защите информационных технологий для базового уровня". Руководство представляет собой гипертекст объемом около 4 МБ (в формате HTML).

В дальнейшем оно было оформлено в виде германского стандарта BSI. В его основе лежит общая методология и компоненты управления информационной безопасностью.

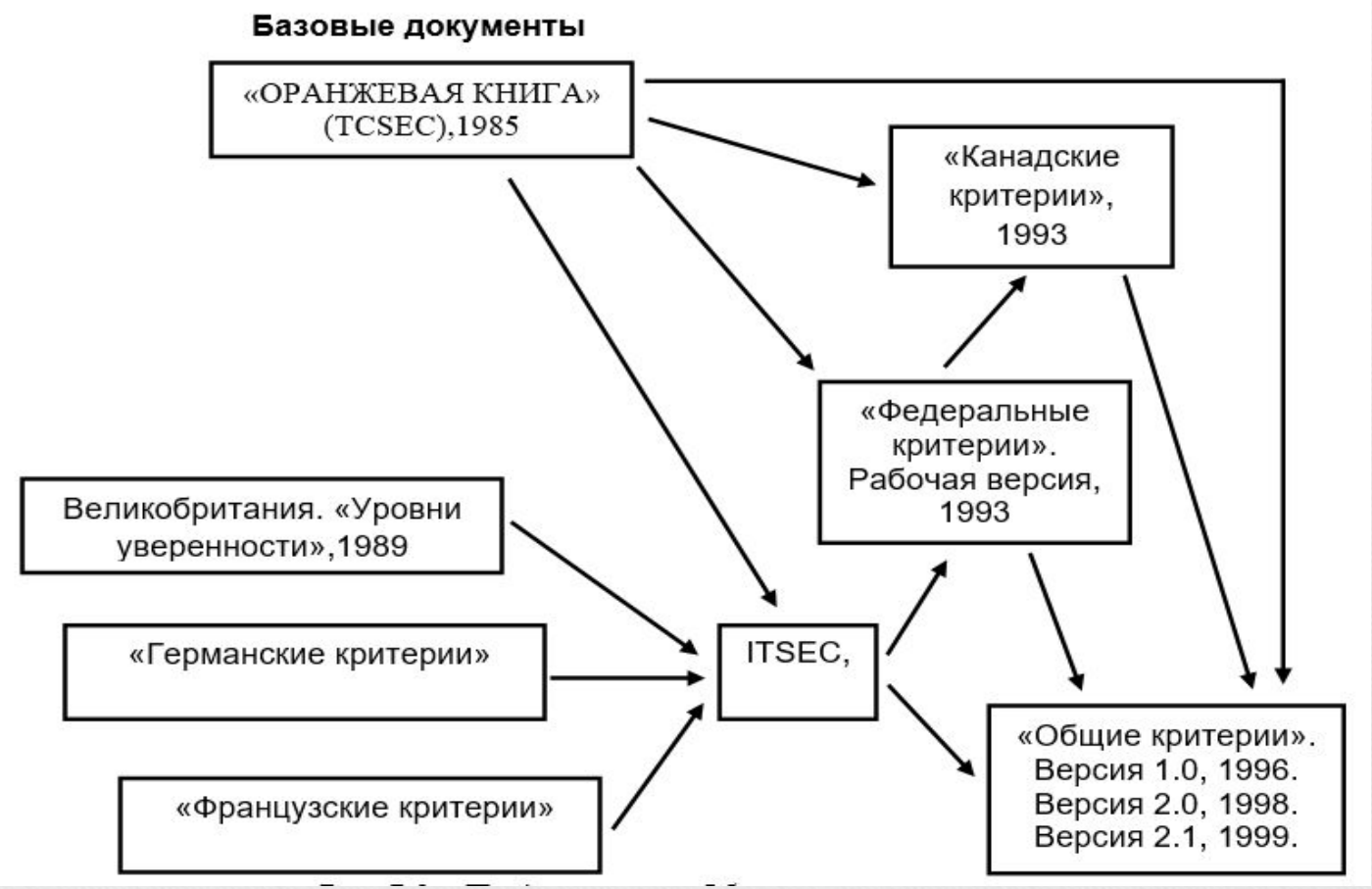
Британский стандарт BS 7799

BS 7799-1:2005 Британский стандарт *BS 7799* «Практические правила управления информационной безопасностью» описывают 127 механизмов контроля, необходимых для построения *системы управления информационной безопасностью* организации, определенных на основе лучших примеров мирового опыта (best practices) в данной области.

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

Международный стандарт ИСО/МЭК 15408-99 (исторически сложившееся название – «Общие критерии») представляет собой наиболее удачный результат обобщения опыта различных государств по разработке и практическому использованию критериев оценки безопасности информационных технологий (ИТ), согласует и развивает целый ряд исходных критериев, а именно существующие европейские, американские и канадские критерии (ITSEC, TCSEC и CTCPEC соответственно).

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"



Национальные стандарты РФ в области ИБ

Национальные стандарты (ГОСТы) в общем случае являются рекомендательными. Основополагающим стандартом РФ в области защиты информации (некриптографическими методами) является ***ГОСТ Р 52069.0-2013 "Защита информации. Система стандартов. Основные положения"*.**

Национальные стандарты РФ в области ИБ

Система стандартов по защите информации включает следующие *виды документов в области стандартизации и защиты информации*, используемых на территории Российской Федерации:

- национальные стандарты Российской Федерации, в том числе ограниченного распространения, государственные военные стандарты, национальные стандарты, оформленные на основе аутентичных переводов международных стандартов (гармонизированные стандарты);
- межгосударственные стандарты;
- правила стандартизации, нормы и рекомендации в области стандартизации;
- общероссийские классификаторы технико-экономической и социальной информации;
- стандарты организаций;
- предварительные национальные стандарты.

Национальные стандарты РФ в области ИБ

На сайте ФСТЭК России приведен перечень стандартов в области защиты информации:

http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty.

Задание:

Необходимо законспектировать данную лекцию, а также рассмотреть и описать один из представленных на сайте стандартов.