Эшелон
комплексная безопасность

Требования по обеспечению безопасности разработки ПО: *Постановка проблемы*

Марков А.С.
канд.техн.наук, ст.науч.сотр., CISSP
НПО «Эшелон»

Актуальность

Объективнее причины

Основная техническая причина всех проблем в области информационной безопасности – наличие уязвимостей в программных средствах

Проблема: кругом одни уязвимости и закладки

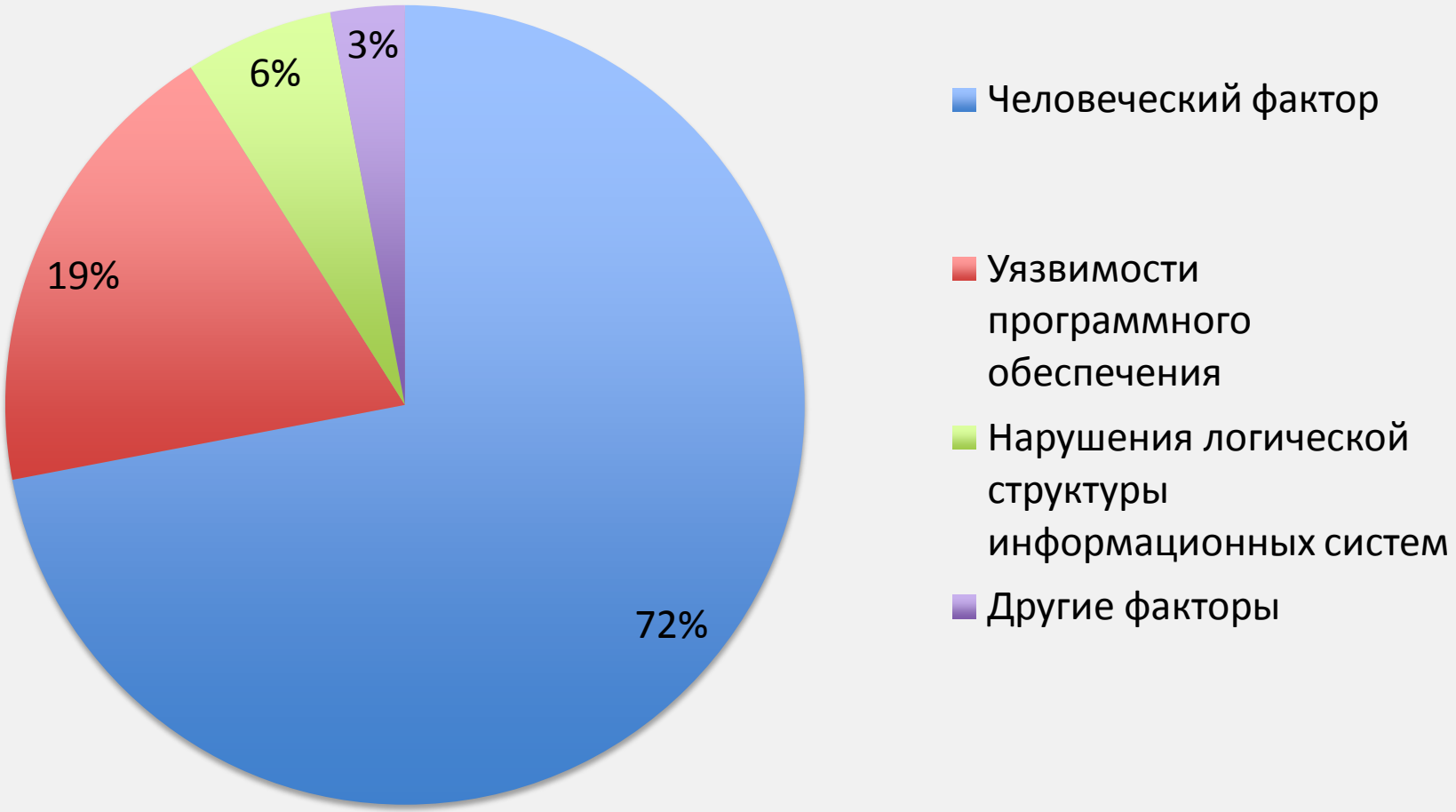
Эшелон
комплексная безопасность

Новости из открытых источников

- В *публичных* скандалах, связанных с наличием закладок были замечены такие компании как:
  - Google
  - Hewlett-Packard
  - Microsoft
  - Actel
  - и др.

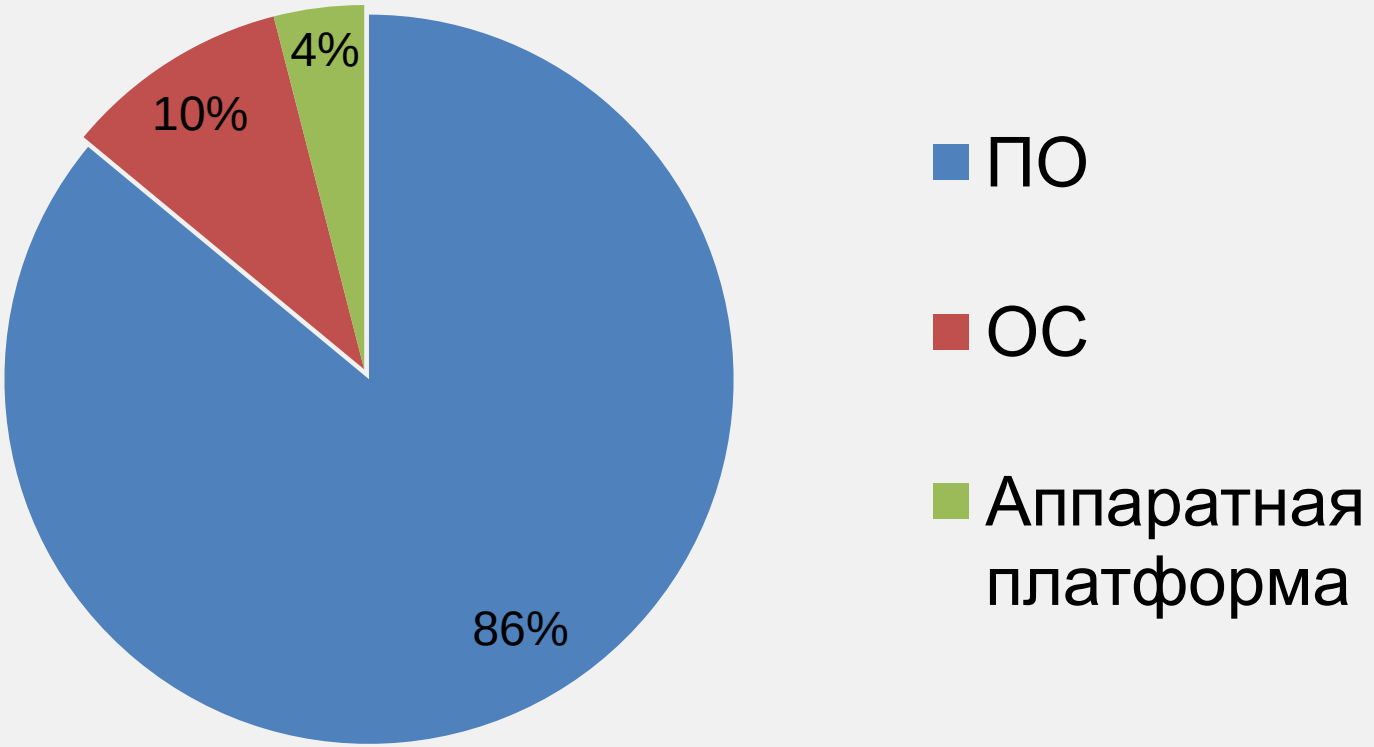
Актуальность проблемы

Факторы, обеспечивающие успешную реализацию компьютерных преступлений



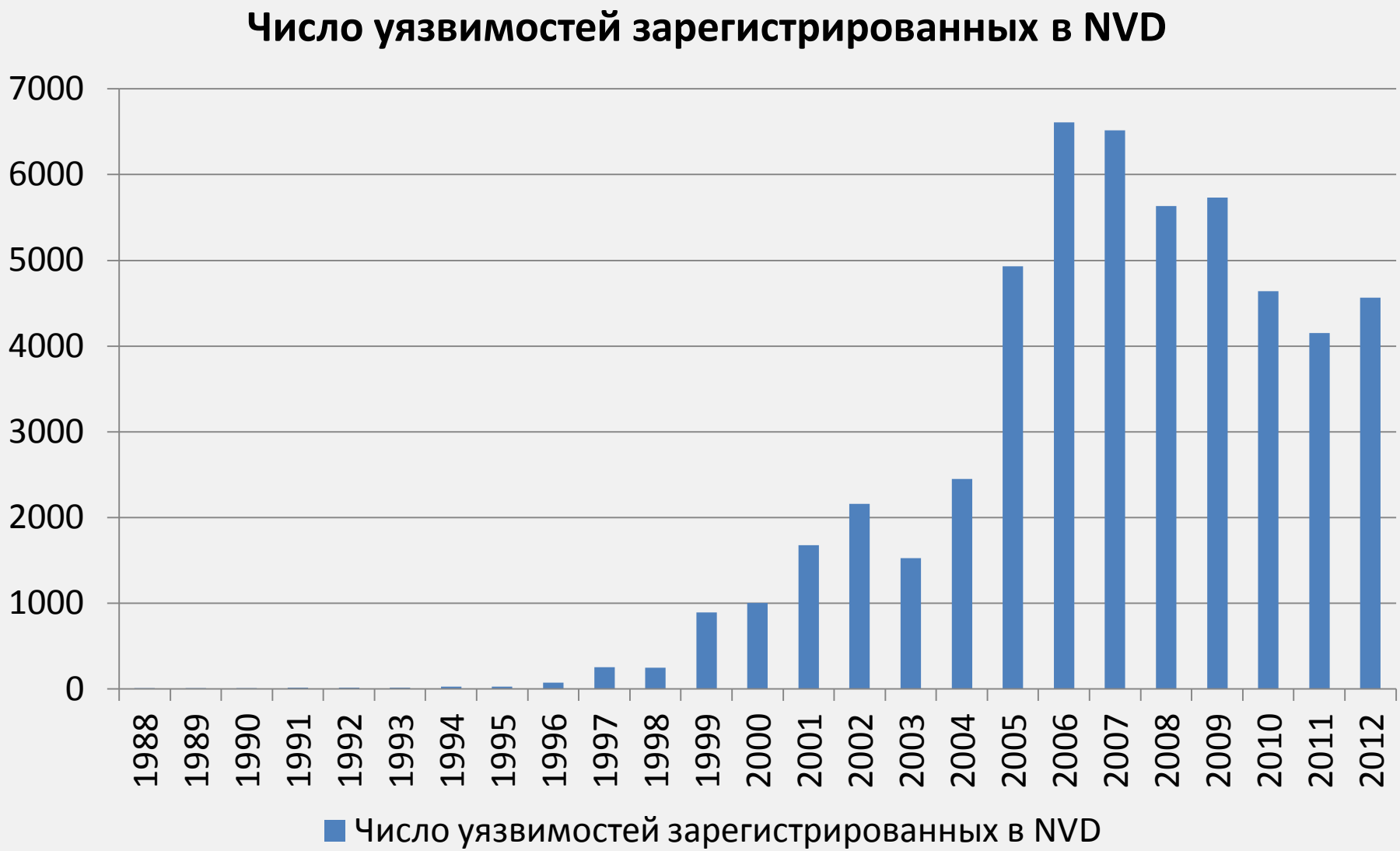
IDC Consulting, 2008

Распределение уязвимостей по источникам



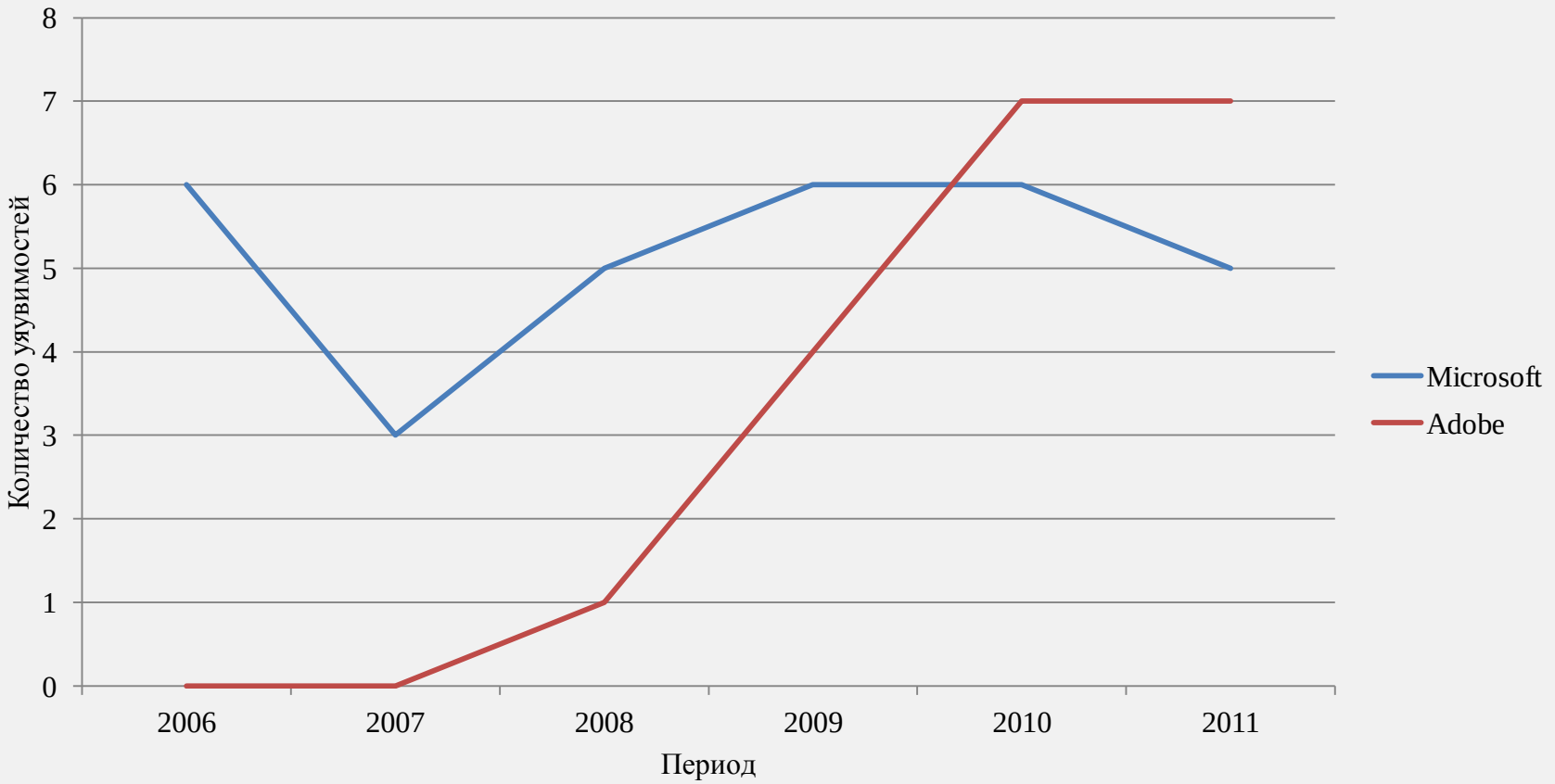
Эшелон
комплексная безопасность

Актуальность проблемы



National Vulnerability Database, 2012

Статистика уязвимостей 0-дня



Качество российского кода

Процент ошибок, выявленных функциональными методами (без структурного анализа)

Стоимость устранения дефектов

Актуальность

Субъективные причины

- Слабая формализация процессов проверки производства (сертификация) и изготовления (лицензирование)
- Ориентация на риск-менеджмент в новых документах ФСТЭК России

Приказ ФСТЭК России № 17

- П.14.4. При определении требований к системе защиты информации ГИС учитываются положения ПБ в случае их разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности.

Приказ ФСТЭК России № 21

П.11. … дополнительно могут применяться следующие меры:

- ✓ проверка на отсутствие НДВ
- ✓ тестирование информационной системы на проникновения;
- ✓ использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием **методов защищенного программирования.**

Безопасное ПС – бездефектная разработка

Безопасное программное средство - ПС, разработанное с использованием процедур безопасной разработки с целью обеспечения конфиденциальности, целостности и доступности обрабатываемой этим ПС информации

Система управления (менеджмента) безопасностью разработки программного обеспечения - часть общей системы управления, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения мер по обеспечению безопасности разработки программного обеспечения

Зачем нужна система менеджмента?

- **Ошибки разработчиков**
  - Отсутствие адекватного анализа рисков ИБ
  - Сложность программного обеспечения
  - Плохой стиль кодирования
  - Недостаточное понимание разработчиками принципов ИБ
  - и т.д.
- **Злой умысел**
  - Заказ иностранных спецслужб
  - «Вредительство»
  - и т.д.

Решение: оценка соответствия

Процессы разработки программного обеспечения

Программное обеспечение

Оценка соответствия ПО в обязательных системах сертификации

ФСТЭК России

ФСБ России

Минобороны России

Эшелон
комплексная безопасность

Системы менеджмента ИБ в за рубежом

Европа, Япония,..	США
Линейка ISO 27000	Акт FISMA-2002

Противоречие СМИБ относительно ПС

- 27000-серия – организационные стандарты
- Оценка безопасности ПО – оценочные стандарты (ГОСТ 15408…)
- 27000-серия – нет конкретных методов безопасной разработки ПО

Процессы безопасной разработки: внедрение и контроль

Международная практика

- ISO 27034
- Microsoft Security Development Lifecycle
- Software Assurance Maturity Model (SAMM)

Российская практика

- Проект стандарта «Требования по обеспечению безопасности разработки ПО»

ISO 27034

- ISO/IEC 27034-1:2011 — Информационные технологии — Безопасность — Безопасность приложений — Обзор и концепты
- ISO/IEC 27034-2 – Нормативы организации
- ISO/IEC 27034-3 – Процесс управления безопасностью приложений
- ISO/IEC 27034-4 – Оценка соответствия
- ISO/IEC 27034-5 – Протоколы и структуры данных

Адаптировать ISO 27034 преждевременно

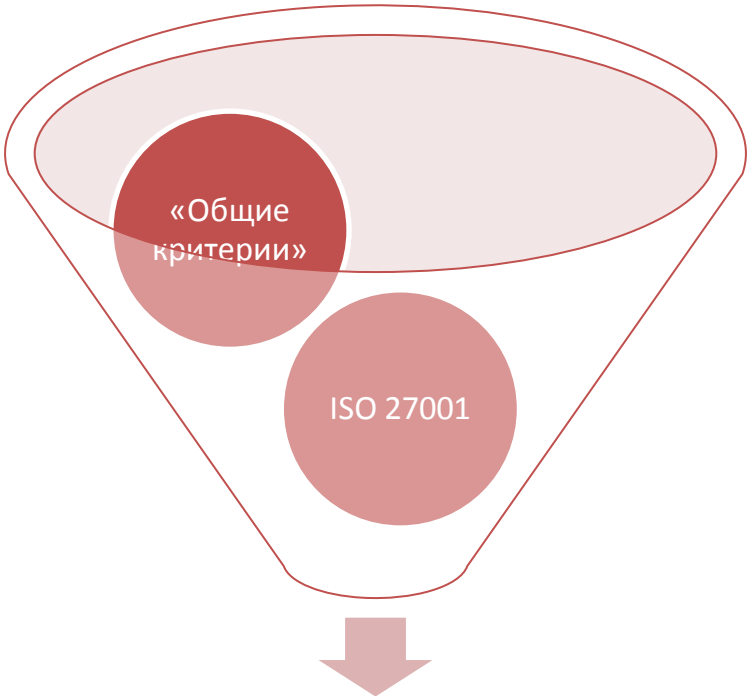
- ✓ Опубликована только первая часть стандарта, остальные будут выпущены в 2015-2017
- ✓ Стандарт содержит довольно общие положения, применение которых на практике без конкретных руководств затруднительно.

Методологии безопасной разработки программ

Характеристика	Методология					
	«Общие критерии»	Microsoft SDL	Open SAMM	Cisco SDL	OWASP CLASP	Руководство «Guidance…»
Обучение специалистов	-	+	+	+	-	-
Обеспечение физической и логической безопасности при разработке ПО	+	-	-	-	-	-
Управление конфигурацией	+	-	-	-	-	-
Моделирование угроз	+	+	+	+	+	-
Определение требований безопасности к разрабатываемому ПО	+	+	+	+	+	-
Использование принципов безопасного проектирования	+	+	+	+	+	+
Анализ исходных кодов ПО	-	+	+	+	+	+
Анализ уязвимостей	+	+	+	+	+	-
Использование методов проектирования безопасного ПО	-	+	+	+	+	-
Обеспечение безопасности поставки	+	-	+	+	-	-

Методы обеспечения безопасности ПО в SDLC

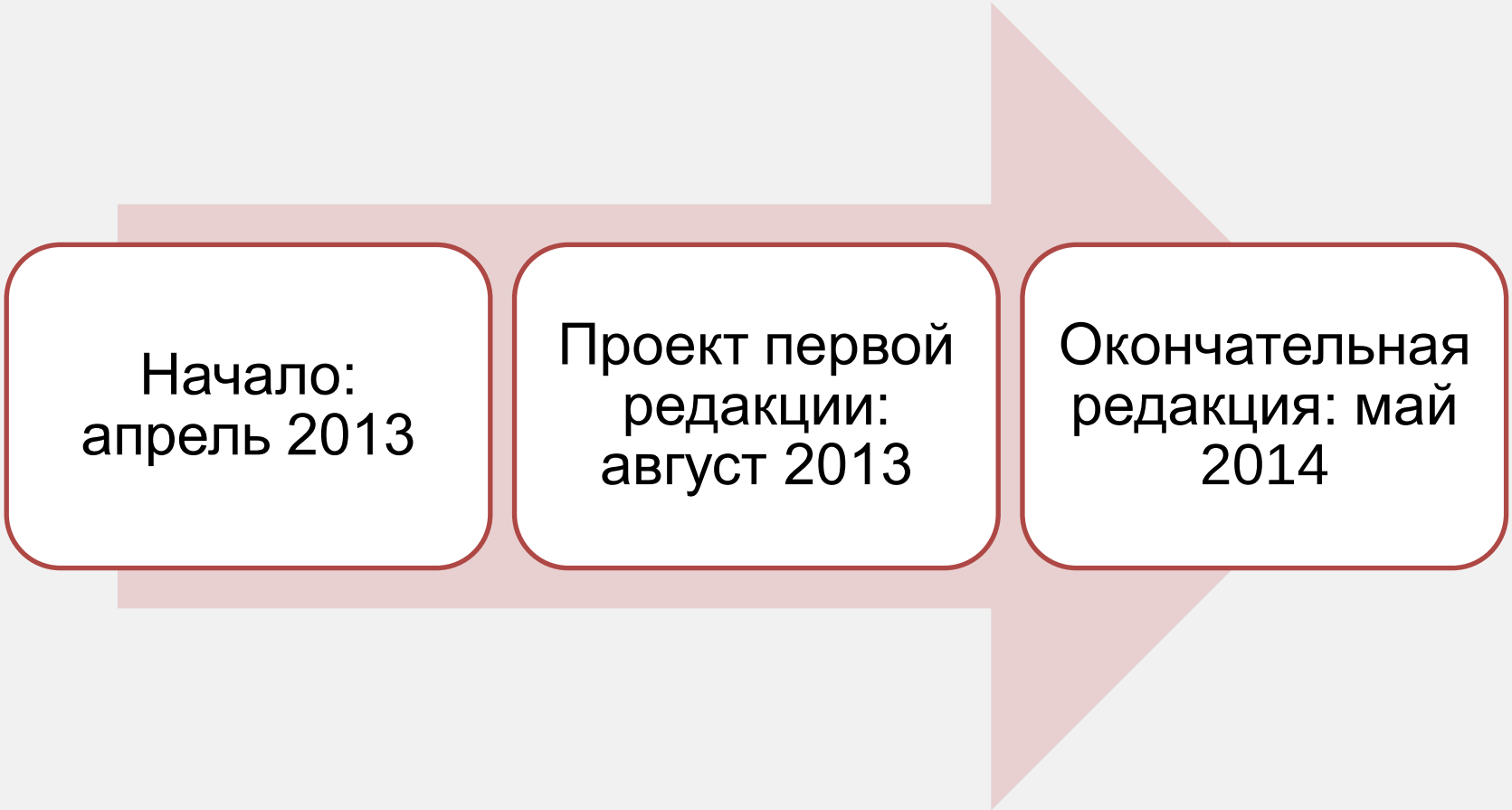
Основная идея разрабатываемого стандарта



Стандарт «Требования по обеспечению безопасности разработки ПО»

Эшелон
комплексная безопасность

ГОСТ Р «Защита информации. Требования по обеспечению безопасности разработки программного обеспечения»



Эшелон
комплексная безопасность

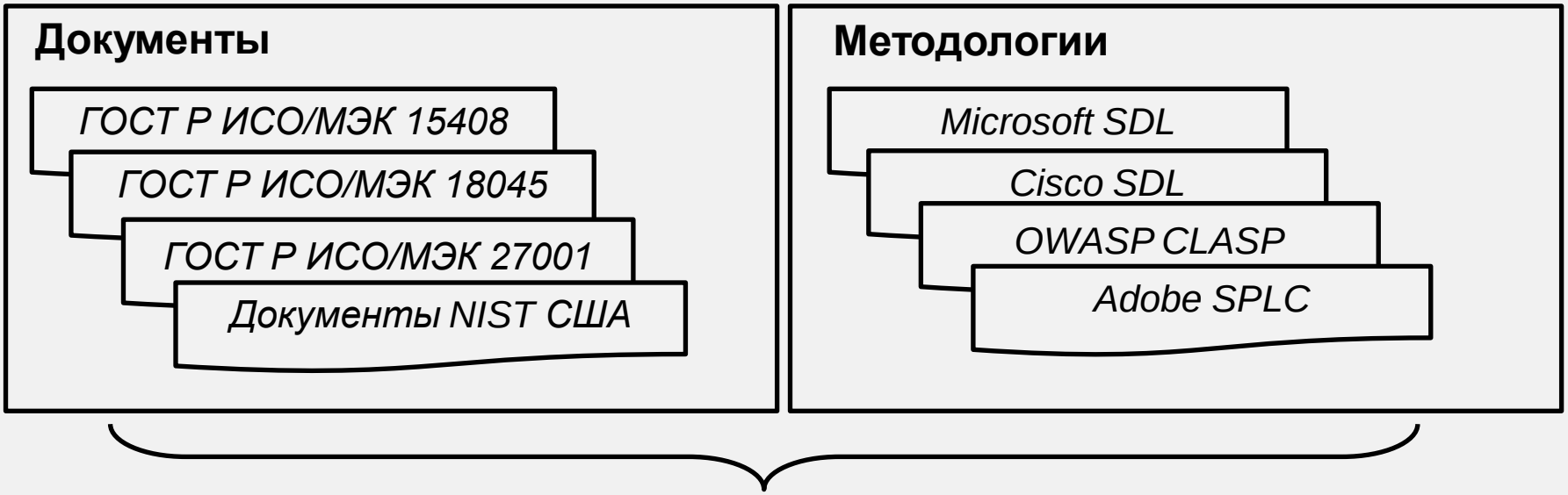
Учитываемые особенности

- обеспечение внедрения необходимых процедур на самых ранних стадиях проектирования программного обеспечения
- учет положений «лучших практик»
- совместимость с методологией «Общих критериев»
- обеспечение возможность интеграции с существующей на предприятии системой управления ИБ

Предлагаемая структура стандарта

- Введение
- Область применения
- Нормативные ссылки
- Термины и определения
- Система обеспечения безопасности разработки программного обеспечения
- Ответственность руководства
- Внутренние аудиты
- Анализ системы обеспечения безопасности разработки со стороны руководства
- Улучшения системы обеспечения безопасности разработки программного обеспечения
- Меры по обеспечению безопасности разработки программного обеспечения

Меры по обеспечению безопасности разработки программного обеспечения



Предлагаемая номенклатура мер:

1. управление конфигурациями
2. безопасная поставка программного обеспечения
3. защита инфраструктуры разработки программного обеспечения
4. использование методов защищенного программирования

Эшелон
комплексная безопасность

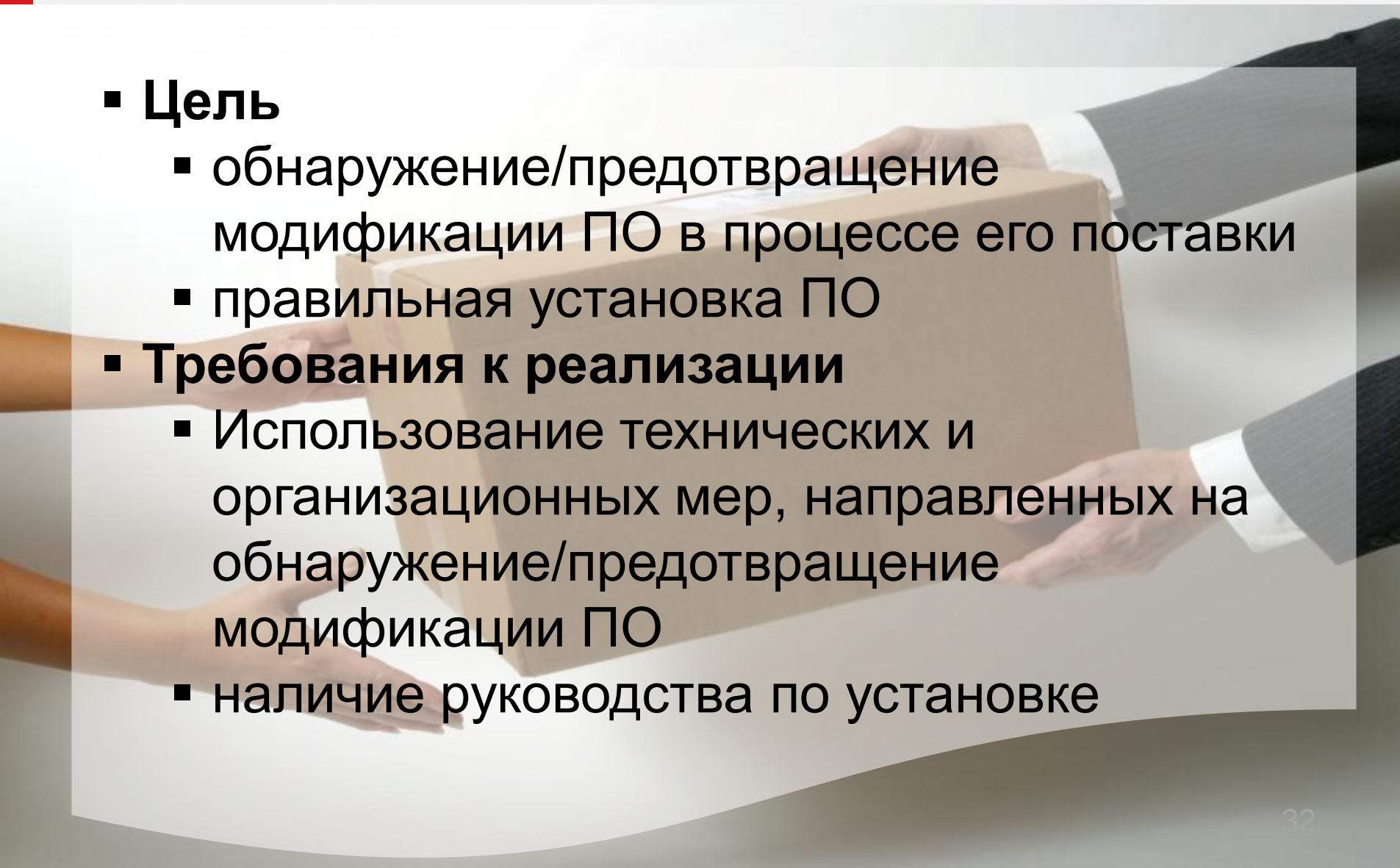
Ключевые процедуры

- управление конфигурациями (разработки)
- безопасная поставка программного обеспечения
- защита инфраструктуры разработки программного обеспечения
- использование методов защищенного программирования.

Управление конфигурациями (разработки)

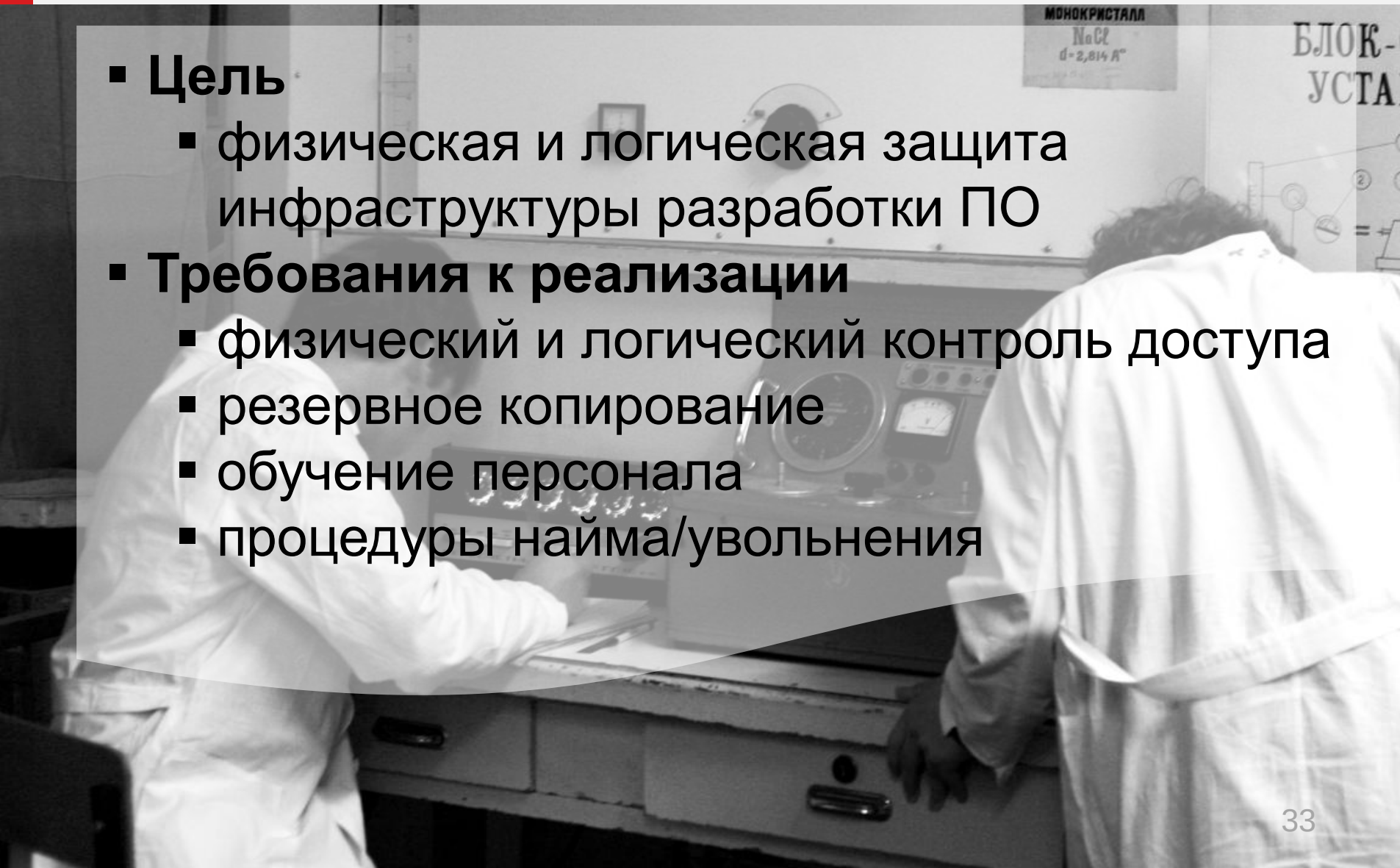
- **Цель**
  - обеспечить корректность и полноту ПО перед его отправкой заказчику
  - предотвращение НСД к элементам конфигурации ПО
- **Требования к реализации**
  - уникальная маркировка ПО
  - идентификация элементов конфигурации
  - использование системы управления конфигурациями

Безопасная поставка программного обеспечения



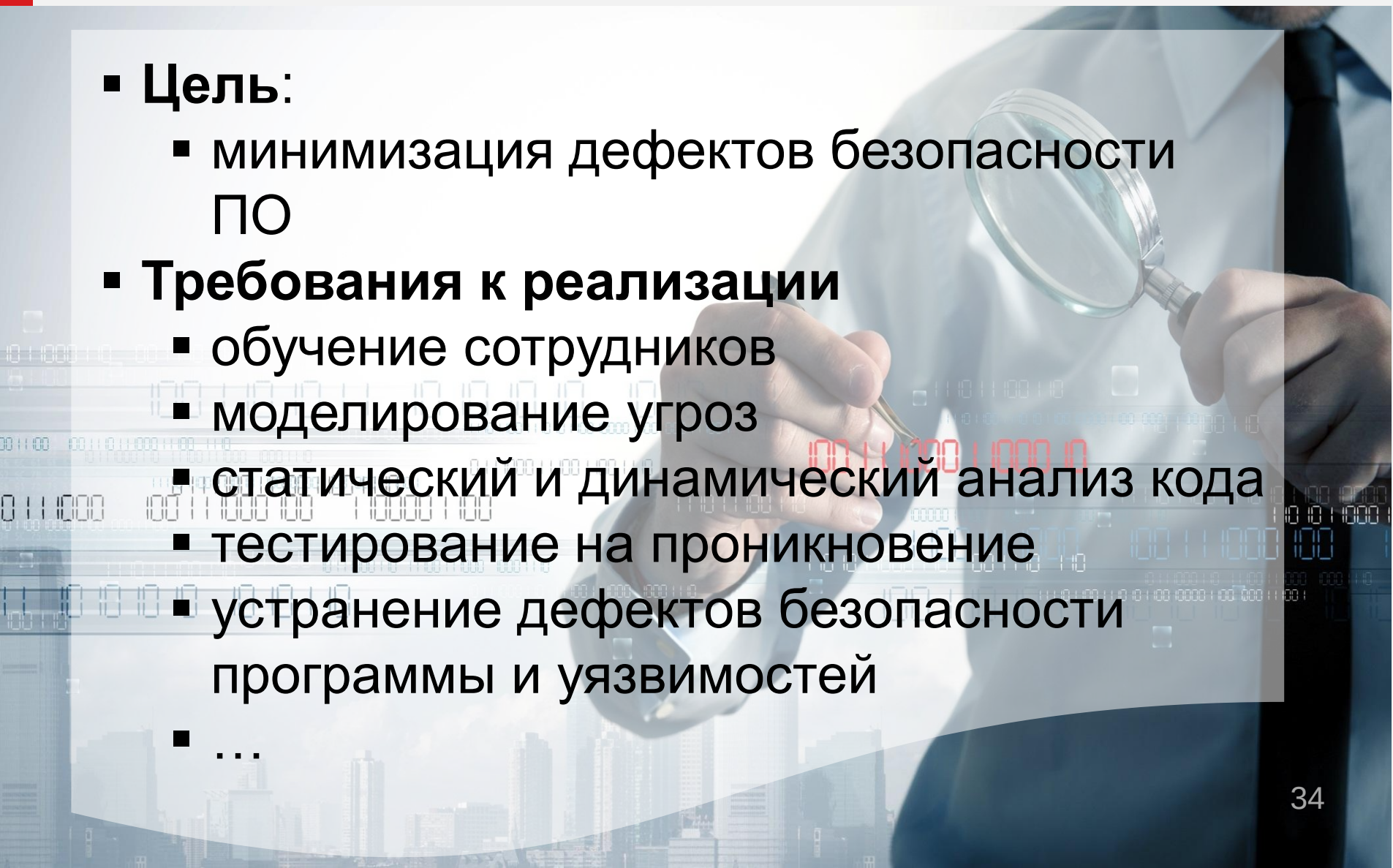
- **Цель**
  - обнаружение/предотвращение модификации ПО в процессе его поставки
  - правильная установка ПО
- **Требования к реализации**
  - Использование технических и организационных мер, направленных на обнаружение/предотвращение модификации ПО
  - наличие руководства по установке

Защита инфраструктуры разработки программного обеспечения



- **Цель**
  - физическая и логическая защита инфраструктуры разработки ПО
- **Требования к реализации**
  - физический и логический контроль доступа
  - резервное копирование
  - обучение персонала
  - процедуры найма/увольнения

Использование методов защищенного программирования



- **Цель**:
  - минимизация дефектов безопасности ПО
- **Требования к реализации**
  - обучение сотрудников
  - моделирование угроз
  - статический и динамический анализ кода
  - тестирование на проникновение
  - устранение дефектов безопасности программы и уязвимостей
  - …

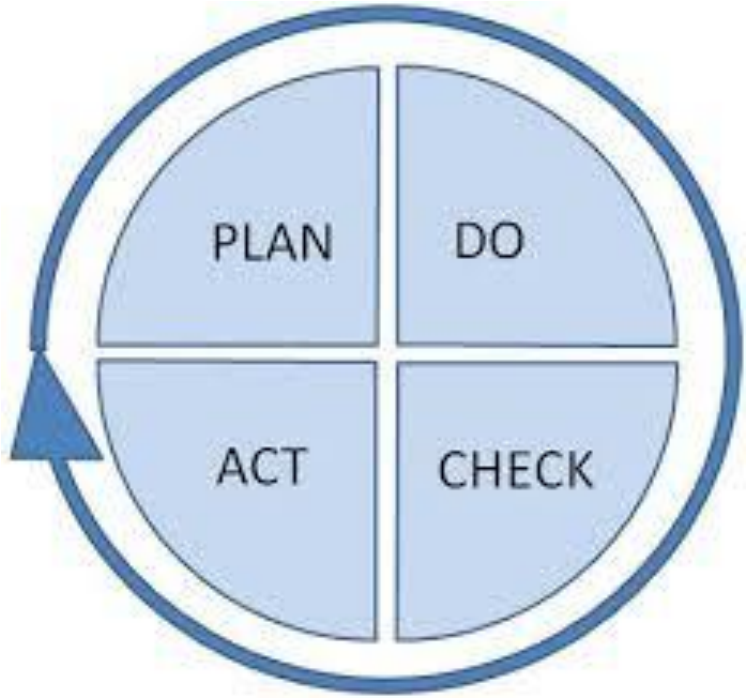
Связь с ГОСТ Р ИСО/МЭК 15408-3

- Поддержка ЖЦ и др.

Требование разрабатываемого стандарта	**Требование ГОСТ Р ИСО/МЭК 15408-3**
Управление конфигурациями	ALC_CMC, ALC_CMS
Безопасная поставка программного обеспечения	ALC_DEL, AGD_PRE
Защита инфраструктуры разработки программного обеспечения	ALC_DVS
Использование методов защищенного программирования	ALC_LCD ALC_TAT ATE_FUN AVA_VAN

Цикл Деминга

Процедуры должны быть не «бумажными», а живыми.



Требования максимально конкретные

- ✓ 5.4.7 Должен проводиться периодический статический анализ исходных кодов ПС с целью выявления уязвимостей и дефектов кода, результаты анализа должны документироваться.
- ✓ 5.8.1 Должна быть реализована процедура, позволяющая выполнять отслеживание и исправление всех ставших известными уязвимостей и дефектов безопасности ПС в каждой версии ПС.
- ✓ 5.8.4 Должна быть реализована процедура анализа влияния обновлений на безопасность ПС, позволяющая определить влияние выпускаемого обновления на функциональные возможности ПС.

Перспективы

- ✓ Рекомендации для производства СЗИ, обеспечивающих разный уровень защищенности
- ✓ Проект ГОСТа – принимаются предложения и замечания

Внедрение подхода позволит

- ✓ Повысить степень технологической безопасности (отечественных) программных продуктов
- ✓ Обеспечить синергетический эффект повышение уровня ИБ систем за счет снижения степени угроз, связанных с типовыми уязвимостями
- ✓ Позволит переосмыслить систему тестирования и испытаний (оценку соответствия) ПО на отсутствие НДВ (в направлении киберугроз)

- ✓ Исключить абстрактные процедуры менеджмента (ISO 9000) и конкретизировать процедуры менеджмента ИБ (ISO 27000)
- ✓ Обеспечить гармонизацию с организационными и оценочными стандартами и учесть «хорошие практики»

- ✓ Исключить элементы субъективизма при лицензировании и сертификации (при серийном производстве)
- ✓ Позволит переосмыслить схемы сертификации

Методы риск-менеджмента ориентированы на повышение эффективности систем по критерию «безопасность-стоимость»

Контактная информация

107023, ул. Электрозаводская, д. 24

+7(495) 223-23-92
+7(495) 645-38-11

http://www.npo-echelon.ru

mail@npo-echelon.ru