DOCFLOW2009
Москва

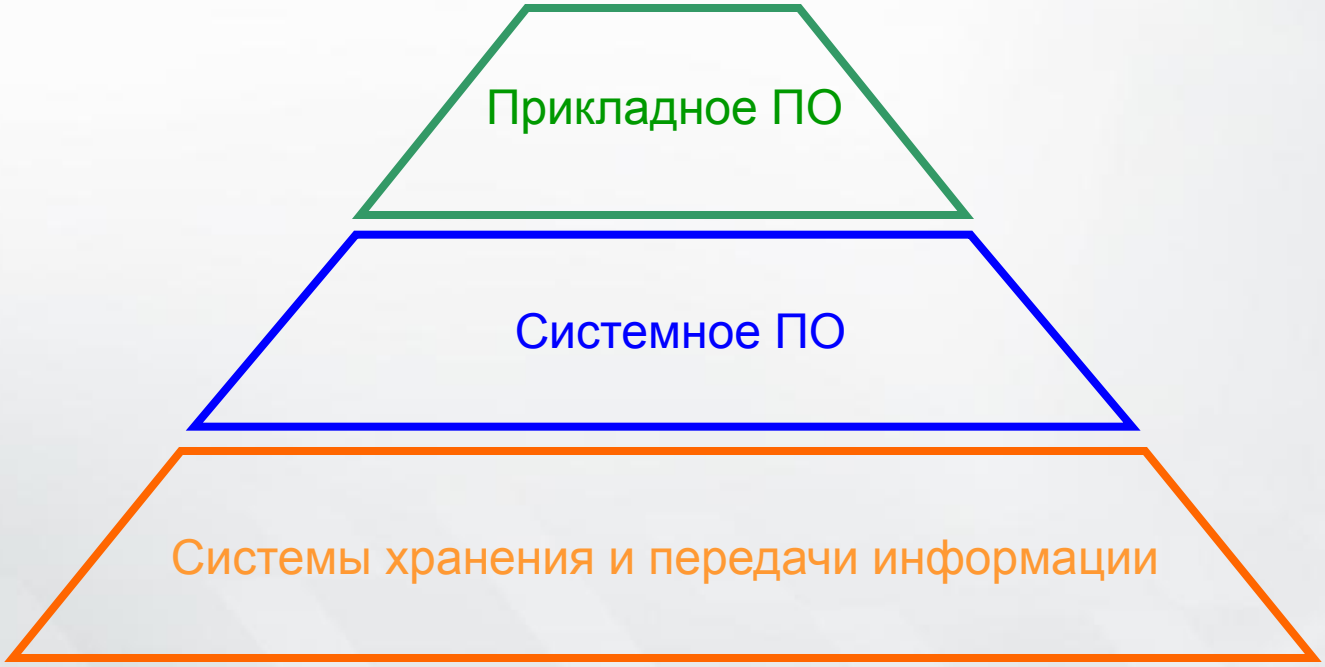
XV юбилейная конференция-выставка по электронному документообороту и автоматизации управления

БОСС референт

Сертификация СЭД на соответствие Закону «О персональных данных»

Алексей Сидак, Центр безопасности информации
Андрей Гриб, компания БОСС-Референт

Область автоматизации



Нормативная база

Федеральный закон от 27 июля 2006 г. №152-ФЗ
«О персональных данных»

Положение об обеспечении безопасности персональных данных
при их обработке в информационных системах персональных данных
(Постановление Правительства РФ от 17.11.2007 г.)

Порядок проведения классификации информационных систем персональных данных
(Приказы ФСТЭК России, ФСБ России, Мининформсвязи России
от 13 февраля 2008 г. № 55/86/20)

+

+

Нормативные документы
ФСТЭК России

Нормативные документы
ФСБ России

Преемственность требований

- Базирование на требованиях апробированных документов:
  - РД АС
  - РД СВТ
  - РД МЭ
  - РД НДВ
  - СТР-К
- Учет уровня развития средств и способов защиты информации:
  - Контроль защищенности
  - Антивирусная защита
  - Расширенные требования по управлению доступом, регистрации, сигнализации о нарушениях защиты

Общая схема подхода к защите персональных данных

Предпроектное обследование

Обследование объекта информатизации как правило является первым шагом на пути внедрения системы защиты персональных данных.

По результатам обследования выдается Отчет об обследовании, показывающий проблемы, препятствующие развертыванию системы защиты персональных данных, а также – пути решения этих проблем.

Классификация системы

- Определение класса системы обработки персональных данных
- Определение **дополнительных** классификационных признаков системы обработки персональных данных

Определение класса системы

По категории обрабатываемых персональных данных:

Категория	Описание
1 Категория	Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.
2 Категория	Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к 1 Категории.
3 Категория	Персональные данные, позволяющие идентифицировать субъекта персональных данных.
4 Категория	Обезличенные и/или общедоступные персональные данные.

Определение класса системы

По объему обрабатываемых персональных данных:

№	Описание
1	В информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом.
2	В информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования.
3	В информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Определение класса системы

Объем Категория	3	2	1
Категория 4	**К4**	**К4**	**К4**
Категория 3	**К3**	**К3**	**К2**
Категория 2	**К3**	**К2**	**К1**
Категория 1	**К1**	**К1**	**К1**

Классификационные признаки

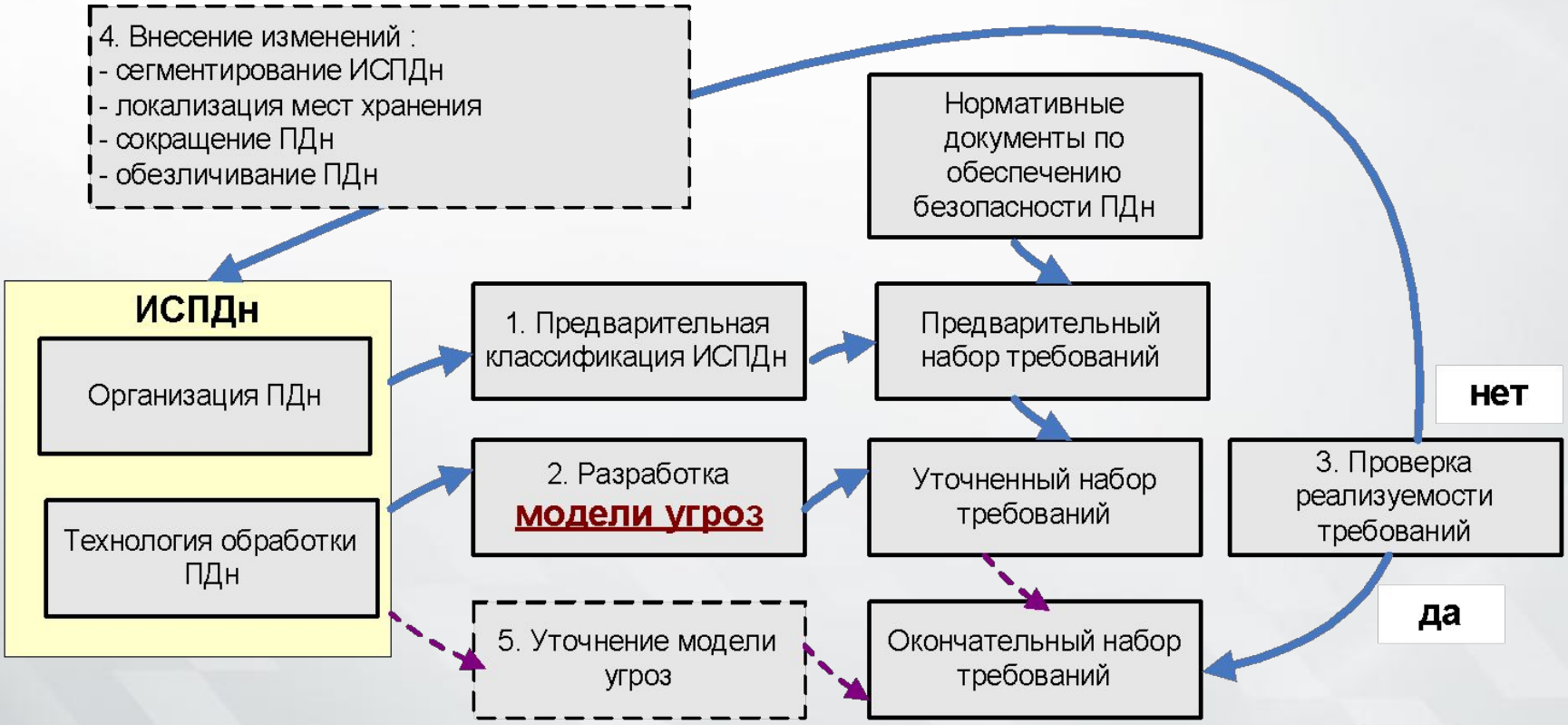
Определяются для каждой конкретной системы согласно Приказам ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

Результат классификации системы

Результатом классификации системы обработки персональных данных является **базовый набор требований** по информационной безопасности.

Базовый набор требований по информационной безопасности уточняется впоследствии по результатам разработки **Модели угроз**.

Модель угроз



Техническое задание

Разработка системы защиты персональных данных осуществляется по Техническому заданию в соответствии с порядком, определённым в СТР-К, нормативных документах ФСТЭК России по обеспечению безопасности персональных данных и национальных стандартах по созданию автоматизированных систем в защищенном исполнении.

Профиль защиты

Профиль защиты представляет собой совокупность минимальных требований для некоторого вида изделий или систем информационных технологий.

Эта конструкция идеально подходит для задания обоснованных требований обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

Проект системы защиты

Включает следующие основные элементы:

- Информационную характеристику объекта защиты
- Требования, предъявляемые к системе защиты персональных данных
- Технические решения по построению системы защиты персональных данных, включая:
  - Структуру и состав системы защиты
  - Проектные решения по системе защиты
  - Спецификацию средств защиты

Встраиваемые функции

Использование встраиваемых в СПО функций позволяет реализовать следующее:

- Управление доступом к персональным данным
- Регистрация доступа к персональным данным
- Учет записей персональных данных
- Сигнализация нарушения защиты персональных данных
- Контроль целостности встроенных средств защиты персональных данных и д.р.

Эффект встраиваемых функций

- Возможность полного контроля персональных данных на уровне записей, полей записей и любых других форм хранения информации
- Сопровождение единым разработчиком
- Сертификационная поддержка
- Возможность построения комплексного решения
- Возможность широкого тиражирования
- Унификация многочисленных систем обработки персональных данных

Состав комплексного решения

- Сертифицированная платформа (ОС, СУБД)
- Сертифицированное СПО со встроенными механизмами защиты
- Изложение организационных мероприятий для объекта информатизации
- Комплект эксплуатационных и организационно-распорядительных документов

Преимущества комплексного решения

- Гарантированное выполнение всех требований по защите персональных данных на множестве типовых объектов
- Возможность использования партнерской сети основных разработчиков для тиражирования решения
- Легкость в модернизации ранее созданных систем обработки персональных данных
- Сокращение стоимости и сроков внедрения в большое количество систем обработки персональных данных

Организационно-технические меры

Организационно-технические меры по обеспечению безопасности персональных данных включают процедуры, регламенты, инструкции, положения которых должны выполняться на объекте информатизации, чтобы обеспечить достаточный уровень контроля и управлять информационной безопасностью.

ОРД

ОРД – организационно-распорядительная документация.

Организационно-распорядительные документы содержат состав и содержание организационно-технических мероприятий по обеспечению безопасности персональных данных на объекте информатизации.

Организационно-распорядительные документы должны быть разработаны до ввода объекта информатизации в эксплуатацию.

Аттестация

Аттестация – процесс подтверждения соответствия системы требованиям по безопасности информации, установленных соответствующими нормативными и руководящими документами регулирующих органов (ФСТЭК России, ФСБ России).

Аттестация

Процесс аттестации информационных систем персональных данных процедурно ничем не отличается от процесса аттестации систем на другие классы защищенности, определяемые руководящими документами ФСТЭК России.

Аттестатом может подтверждаться соответствие системы одновременно нескольким классам, например, классу 1Г в соответствии с РД АС и классу К3 для информационных систем персональных данных.

Пример Аттестата соответствия

2

1. Настоящим **АТТЕСТАТОМ** удостоверяется, что:
Автоматизированная информационная система …….. - «АС …» соответствует требованиям нормативной документации по безопасности информации в части защиты от несанкционированного доступа по классам защищенности:
класс **1Г** – в соответствии с классификацией Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
класс **К3** – в соответствии с Порядком проведения классификации информационных систем персональных данных (утвержден приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20).
Состав технических и программных средств **АС …** представлен в Техническом паспорте на Автоматизированную информационную систему ……..
2. Организационная структура, уровень подготовки специалистов, обеспечивают поддержание уровня защищенности **АС …** в процессе эксплуатации в соответствии с установленными требованиями.
3. Аттестация **АС …** выполнена в соответствии с “Программой и методикой аттестационных испытаний... ”, утвержденной Председателем Центра безопасности информации ___ ноября 2008 г.
4. С учетом результатов аттестационных испытаний в **АС ….** разрешается обработка конфиденциальной информации.
5. При эксплуатации **АС ….** запрещается без согласования с органом по аттестации:
изменять состав технических и программных средств, входящих в **АС ….**;
изменять установленный порядок доступа персонала к циркулирующей в **АС …** служебной и конфиденциальной информации и режим допуска лиц в помещения с оборудованием **АС ….**;
осуществлять другие технические и организационные мероприятия, которые могут создать предпосылки для утечки защищаемой информации за счет несанкционированного доступа к информации.
6. Контроль за эффективностью реализованных мер и средств защиты возлагается на ответственных за обеспечение информационной безопасности **АС ….**
7. Подробные результаты аттестационных испытаний приведены в “Заключении по результатам аттестационных испытаний на соответствие требованиям по безопасности информации **Автоматизированной информационной системы ……**

3

- «АС …» от ___ декабря 2009 г.
8. «Аттестат соответствия» выдан сроком на 3 года, в течение которого должна быть обеспечена неизменность условий функционирования АС …..
9. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации:
состав и размещение технических и программных средств АС ….;
состав и настройки установленных в АС ….. средств защиты от несанкционированного доступа к информации;
изменения в технологическом процессе обработки информации в АС ……
Руководитель аттестационной комиссии

_____

“__“ января 2009 г.

Персональные данные в системах электронного документооборота

БОСС референт

- Обработка обращений граждан
- Электронные административные регламенты и оказание госуслуг
- Обработка заявлений физических лиц в коммерческих организациях
- Данные о сотрудниках организации в модуле «Справочник организации»

Оценка класса ИСПДн для систем электронного документооборота

БОСС референт

Объем Категория	3	2	1
Категория 4	**К4**	**К4**	**К4**
Категория 3	**К3**	**К3**	**К2**
Категория 2	**К3**	**К2**	**К1**
Категория 1	**К1**	**К1**	**К1**

Распределение функций безопасности с системах электронного документооборота

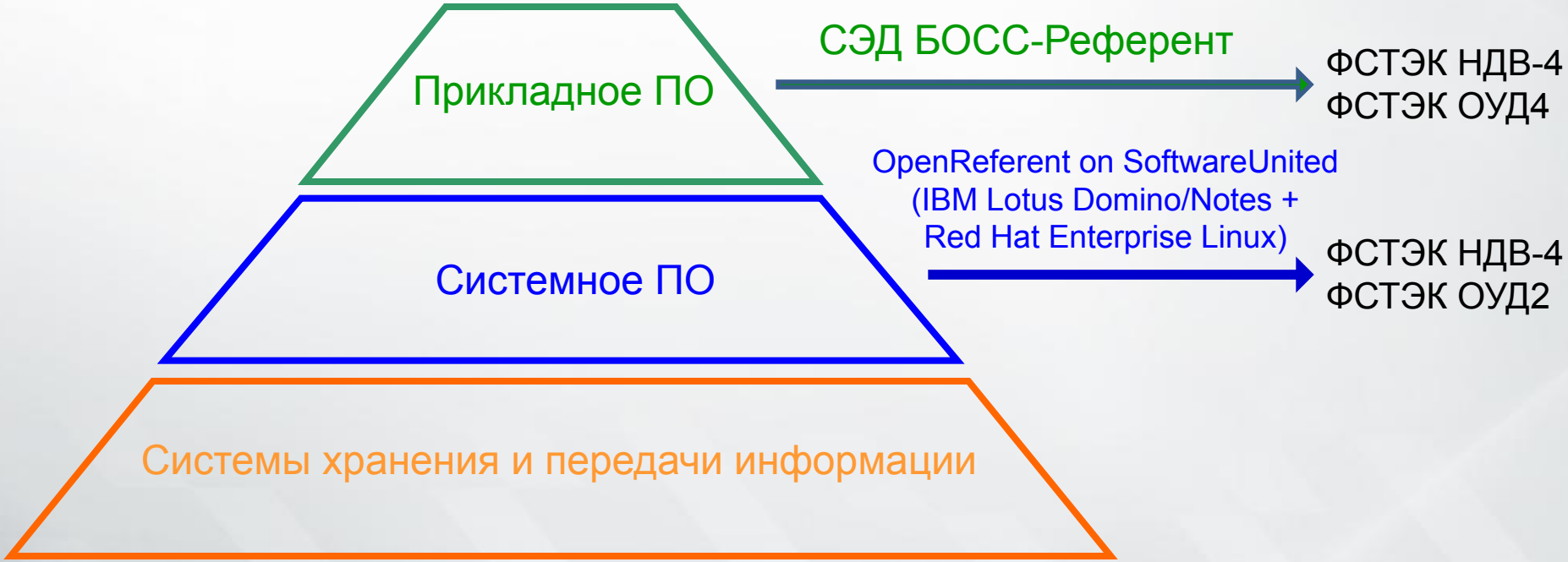
БОСС референт

Аудит безопасности (FAU)
Защита данных пользователей (FDP)

Идентификация и аутентификация (FIA)
Управление безопасностью (FMT)
Защита ФБО (FPT)
Доступ ОО (FTA)

Структура сертификации системы электронного документооборота на примере СЭД «БОСС-Референт»

БОСС референт



Сертификат ОУД (ФСТЭК)

БОСС референт

Официальное наименование:

«Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», (Гостехкомиссия России, 2002 г.) – для оценочного уровня доверия

Уровни: от 1 до 7

Что проверяется на сертификационных испытаниях:

- уровень защищенности ПО
- корректность работы функций безопасности

Сертификат НДВ (ФСТЭК)

БОСС референт

Официальное наименование:

«Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999 г.)

Уровни: от 4 до 1

Что проверяется на сертификационных испытаниях:

- Отсутствие «черных ходов» в программном коде

Сведения, предоставляемые разработчиком на сертификационные испытания

БОСС референт

ОУД

- Задание по безопасности - основной документ, содержащий описание функций ПО в части безопасности.
- Описание проектных решений, относящихся к реализации функций безопасности ПО.
- Тесты, используемые разработчиком для проверки функций безопасности, и подтверждения, что используемые тесты покрывают весь заявленный функционал безопасности.
- Эксплуатационная документация.

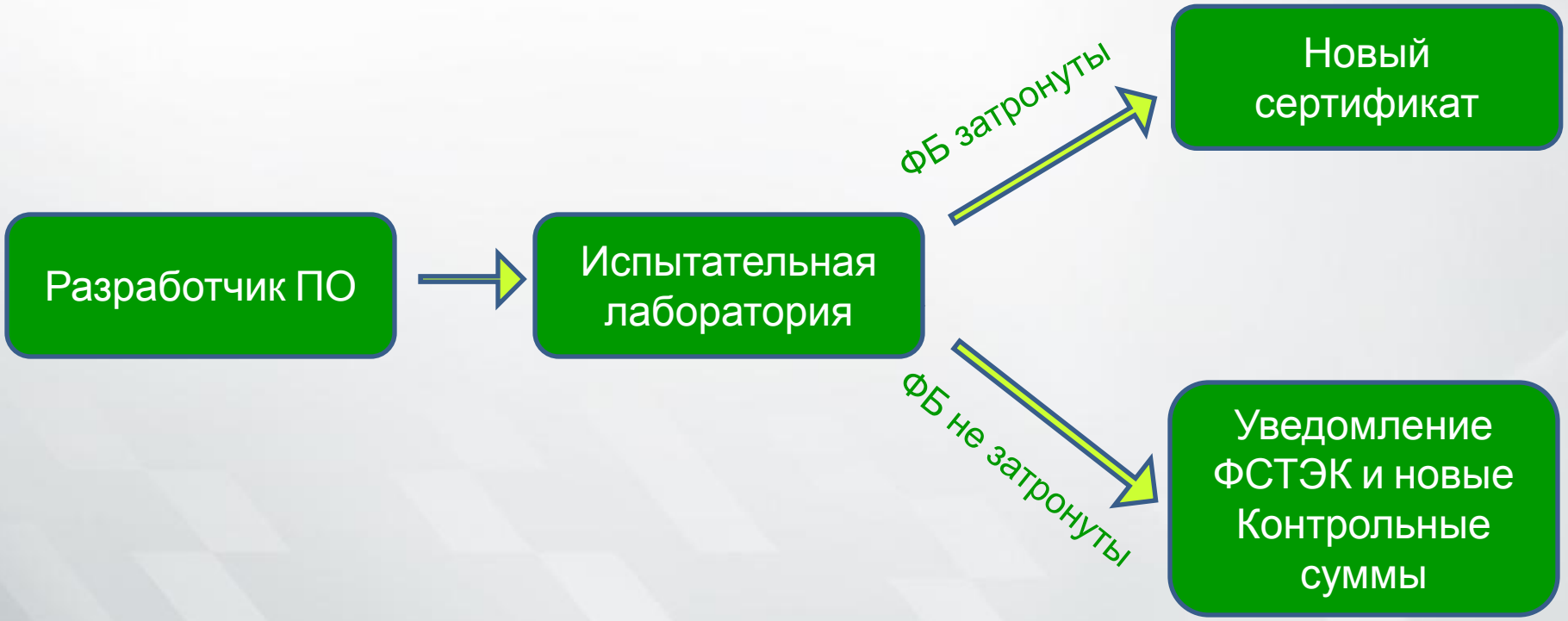
НДВ

- Исходные тексты продукта.
- Описание, из каких компонент состоит продукт до уровня отдельного исполняемого файла.
- Описание того, из каких файлов с исходными текстами собираются исполняемые файлы продукта.
- Описание процедур сборки из исходных текстов дистрибутива, предоставляемого конечным пользователям. Получающийся в результате сборки дистрибутив должен совпадать с тем, который распространяется разработчиком.

Версионность сертифицированных программных продуктов

БОСС референт

При выпуске обновлений сертифицированного ПО проводится инспекционный контроль:



Производство сертифицированных программных продуктов

БОСС референт

Производство Комплектов сертифицированного ПО – процедура верификации дистрибутивов ПО, находящегося на физических носителях инсталляционного комплекта ПО и формирования Комплекта сертифицированного ПО.

Комплект сертифицированного ПО:

- Верифицированный инсталляционный комплект ПО
- Эксплуатационная документация ПО, включая Руководство по безопасной настройке и контролю сертифицированного ПС
- Формуляр на сертифицированное ПС
- Лицензионное свидетельство ПС
- Набор информационных материалов

Способы производства сертифицированного ПО:

- Серийное производство (требуется аттестация производства)
- Партия
- Единичный экземпляр

Спасибо за внимание!

Алексей Сидак

Директор департамента систем информационной безопасности

Кандидат технических наук

Sidak@cbi-info.ru

141090, Московская обл.,

г. Юбилейный

ул. Пионерская, д. 1/4

тел. (495) 543-30-60

www.cbi-info.ru

БОСС референт

Андрей Гриб

Генеральный директор

AGrib@boss-referent.ru

117218,

г. Москва,

ул. Кржижановского, д.21а

тел. (495) 785-53-59

www.boss-referent.ru