РОСАТОМ

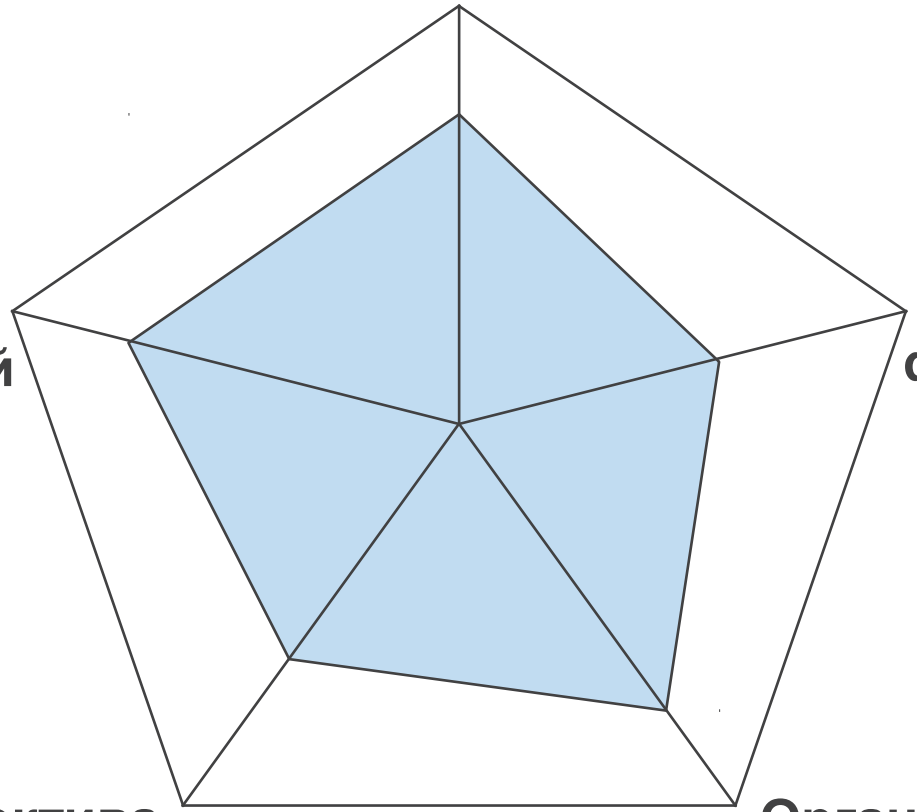
ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

Проблемы информационной безопасности при создании АСЗИ

В.И.Будников, Э.Н.Васильев

Факторы успеха для внедрения информационных систем

Необходимый и достаточный функционал программного обеспечения



Выполнение требований информационной безопасности

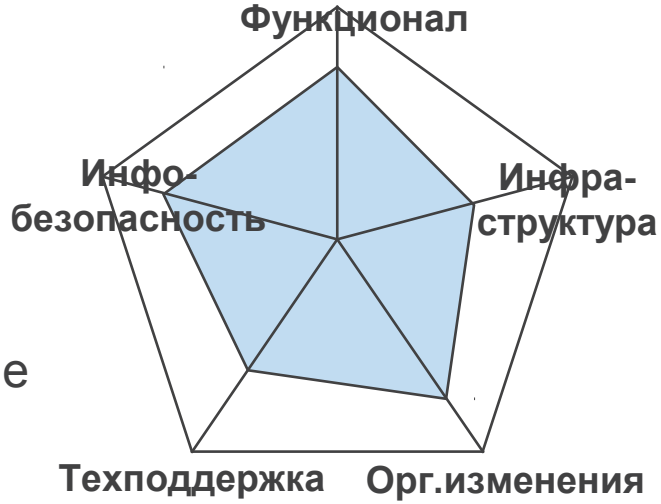
Инфраструктура для функционирования информационных систем

Создание коллектива и правил техподдержки внедряемой системы

Организационные изменения – ломка традиций у руководителей и сотрудников

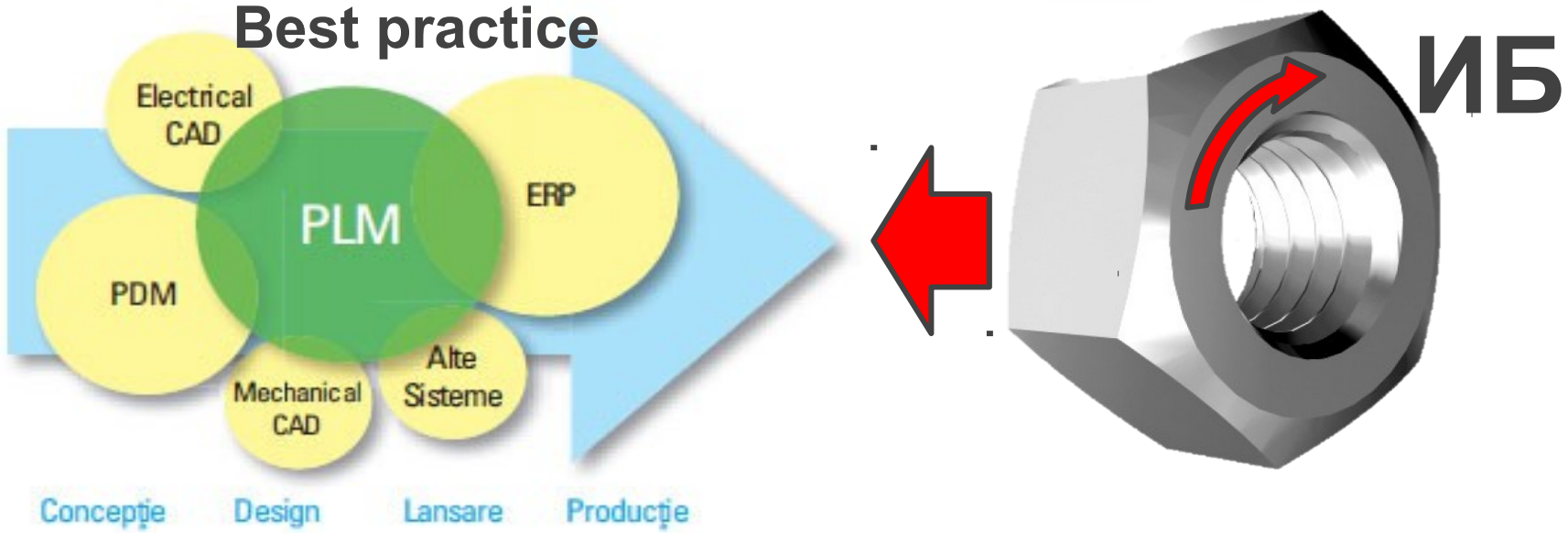
Кто и как руководит автоматизацией деятельности предприятия

1. **Кого назначают руководить автоматизацией?**
   Варианты:
   •Проектировщика (конструктора)
   •Программиста (специалиста в ВТ)
   •Специалиста в финансово-экономических вопросах
   •Ответственного за стратегическое планирование
   •Представителя службы главного-инженера
   и т.д.



2. **Как руководитель действует?**
   1)Проводит анализ того, что есть на предприятии (системы, специалисты, предпочтения, опыт)
   2)Ездит по аналогичным предприятиям и знакомится с их опытом (ИТ-туризм)
   3)Привлекает интеграторов
   4)Сосредотачивается на вопросах функционала и инфраструктуры.

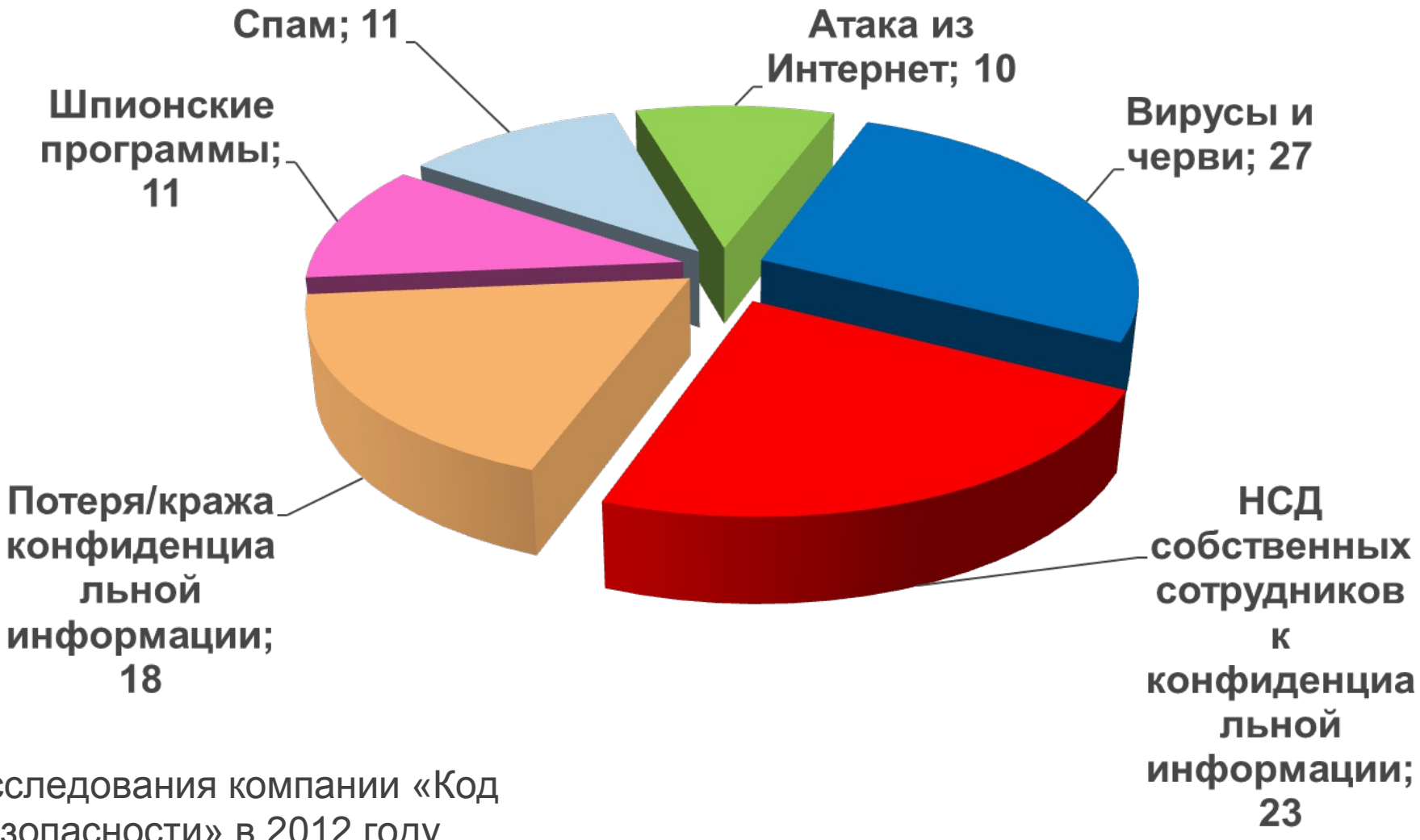
Типичное заблуждение «автоматизаторов»: Систему информационной безопасности можно «накрутить» на готовые информационные системы предприятия



Чаще всего в погоне за функционалом и инфраструктурой автоматизаторы действуют исходя из «Лучших практик», исследуют ПО, нанимают консалтинг, организовывают обучение, оставляя вопросы ИБ на «потом».

В результате, когда деньги потрачены и система функционально готова, оказывается, что ее невозможно запустить по требованиям ИБ.

Как видят угрозы информационной безопасности российские предприятия (%)



Исследования компании «Код безопасности» в 2012 году

Определим, о безопасности какой информации мы говорим

Виды информации по степени конфиденциальности/ секретности		Чем регламентируется	Как определяется принадлежность к данному виду информации
Несекретная	**Для открытого опубликования**	-	По остаточному принципу
	Для служебного пользования	Постановление правительства РФ в редакции от 20.07.12 №740, отраслевые нормативные акты	Отраслевые перечни служебной информации
	Персональные данные	Федеральный закон №152-ФЗ от 27.07.2006 (в последней ред.)	Определена законодательно
	Коммерческая тайна	Федеральный закон №98-ФЗ от 29.07.2004 (в последней ред.), отраслевые нормативные акты	Отраслевые перечни коммерческой тайны и перечни КТ предприятий
Гостайна с разными уровнями секретности		Федеральный закон №131-ФЗ от 21.07.1993 (в последней ред.), регламентирующие документы ФСТЭК, ФСБ, МО, отраслевые нормативные акты	Государственные и отраслевые перечни сведений, подлежащих засекречиванию

Перечислим возможные способы защиты информации (по ГОСТ Р 50922-2006)

Вид защиты	Определение
Правовая защита информации	Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов, регулирующих отношения субъектов по защите информации, применение этих документов, а также надзор и контроль за их исполнением
Техническая защита информации	Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации, подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств
Криптографическая защита информации	Защита информации с помощью ее криптографического преобразования
Физическая защита информации	Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

Кто и как определяет требования к методам защиты информации

В Российской Федерации законодательно определена система государственной защиты информации, полномочия и обязанности в которой разграничены между различными структурами и ведомствами.

На Федеральную службу по техническому и экспортному контролю (ФСТЭК России) возложены, в т.ч., следующие функции:

- **обеспечение безопасности информации** (некриптографическими методами) в информационной и телекоммуникационной инфраструктуре, оказывающих существенное влияние на безопасность государства в информационной сфере;
- определение методов (некриптографических) защиты информации, **содержащей государственную тайну и иной информации с ограниченным доступом**.

Согласно нормативным документам ФСТЭК, информация ограниченного распространения должна обрабатываться в **автоматизированных системах в защищенном исполнении (АСЗИ).**

Требования ИБ меняются от уровня конфиденциальности информации и прав доступа пользователей к ней

Вся информация не выше ДСП	3Б	2Б	1Г
Вся информация секретная	3А	2А	1В
Вся информация совсекретная	3А	2А	1Б
Информация различных грифов от ДСП до СС	2А	2А	1Б
	Пользователь один, ему доступна вся информация	Пользователей много вся информация доступна всем пользователям	Доступ к информации разграничен по группам пользователей или отдельным пользователям

Определение класса и требований к проектируемой АСЗИ «по ФСТЭК» – циклическая попытка ответить на несколько вопросов

Залог успешного использования информационных систем – консолидация данных о проекте в едином информационном пространстве

1) В любом секретном проекте абсолютное большинство информации – несекретное или служебное, но общий гриф проекта определяется по максимальному грифу отдельных объектов информации

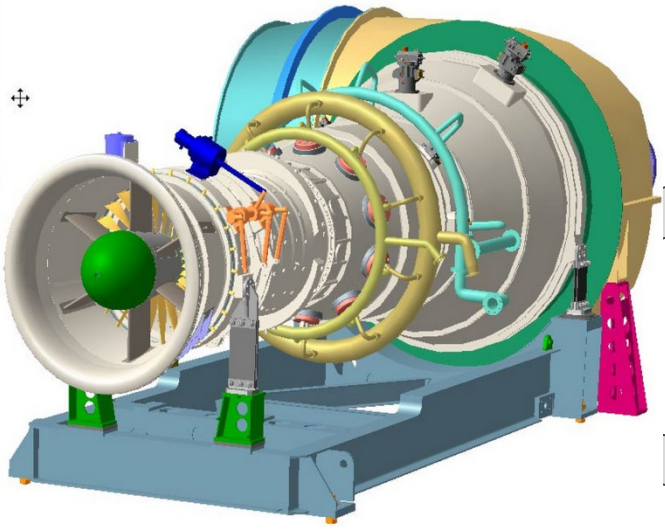
2) Все современное программное обеспечение для управления проектными данными (напр. конструирование, строительство, экономика, планирование и т.д.) ориентировано на управление и автоматизированную обработку всей совокупности связанных между собой данных.

3) Разделение информации проекта по разным АС в зависимости от степени конфиденциальности приведет к резкому снижению эффективности (до полной невозможности) использования ПО за счет потери связей между проектными данными, неоправданным потерям на синхронизации данных, дублированию и ошибкам

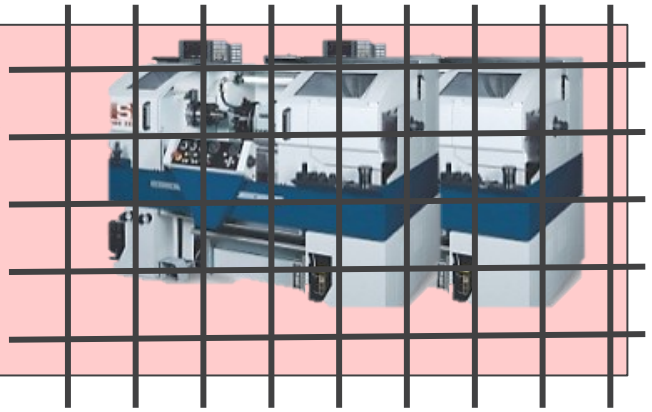
Особенности передачи электронной КД от разработчиков на производство

Разработка КД идет в едином информационном пространстве, все изделие должно быть собрано в одном месте.

Но на производстве комплект КД разбивается на части:



10-20% КД на участок для обработки гостайны



80-90 % КД на несекретный участок

Особенности определения перечня информации и максимального ее грифа в АСЗИ

Бумажные документы в шкафу	Электронные документы в АСЗИ
1) Гриф каждого документа рассматривается независимо. 2) Несколько ДСП документов спокойно могут лежать в шкафу, даже если они в сумме содержат секреты 3) О грифе по совокупности нужно говорить только при физическом сшивании нескольких документов, например, в дело.	1) Кроме грифа отдельных электронных документов, есть еще гриф носителя данных 2) Данные на носителях в АСЗИ должны рассматриваться в совокупности (по аналогии с документами, вшитыми в одно дело) 3) Несколько электронных документов уровня ДСП, имеющих связь, в АСЗИ могут превратиться в секретные данные.

Особенности определения перечня информации и максимального ее грифа в АСЗИ

Для определения максимального грифа информации, обрабатываемой в АСЗИ, нужно:

1) Определить **перечень информации**, обрабатываемой в АСЗИ, где каждый отдельный документ не превышает выбранного уровня конфиденциальности/секретности
2) На основе анализа этого перечня дать **заключение о максимальном уровне** конфиденциальности/секретности информации «по совокупности».
3) При необходимости **наложить ограничения** (запрет) на обработку отдельных видов информации в АСЗИ, чтобы не произошло превышение разрешенного уровня.

Технология обработки информации – важнейший документ в АСЗИ

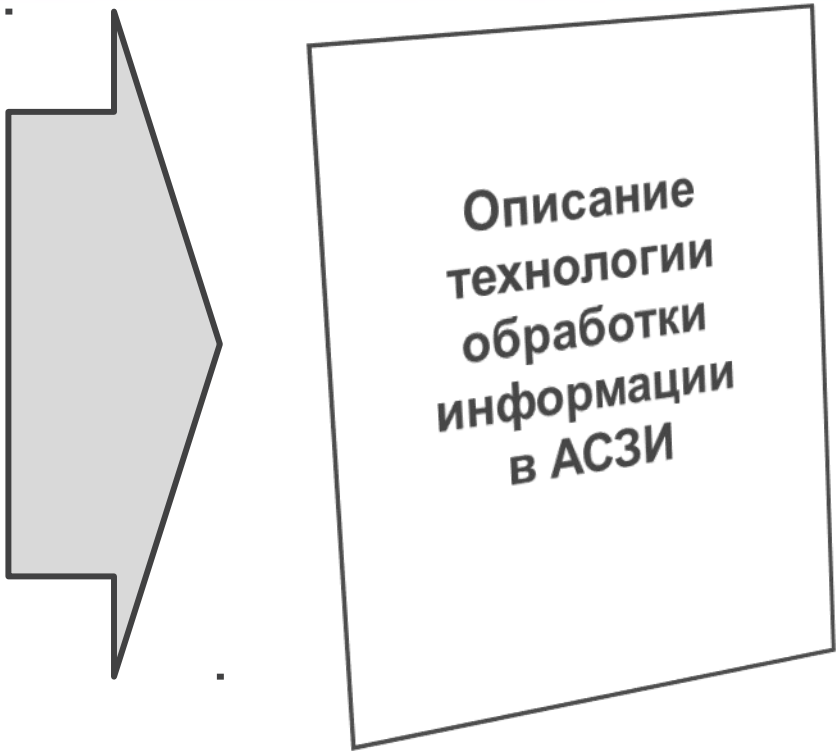
Перечень защищаемых ресурсов

+

Перечень ПО, допущенного в АСЗИ

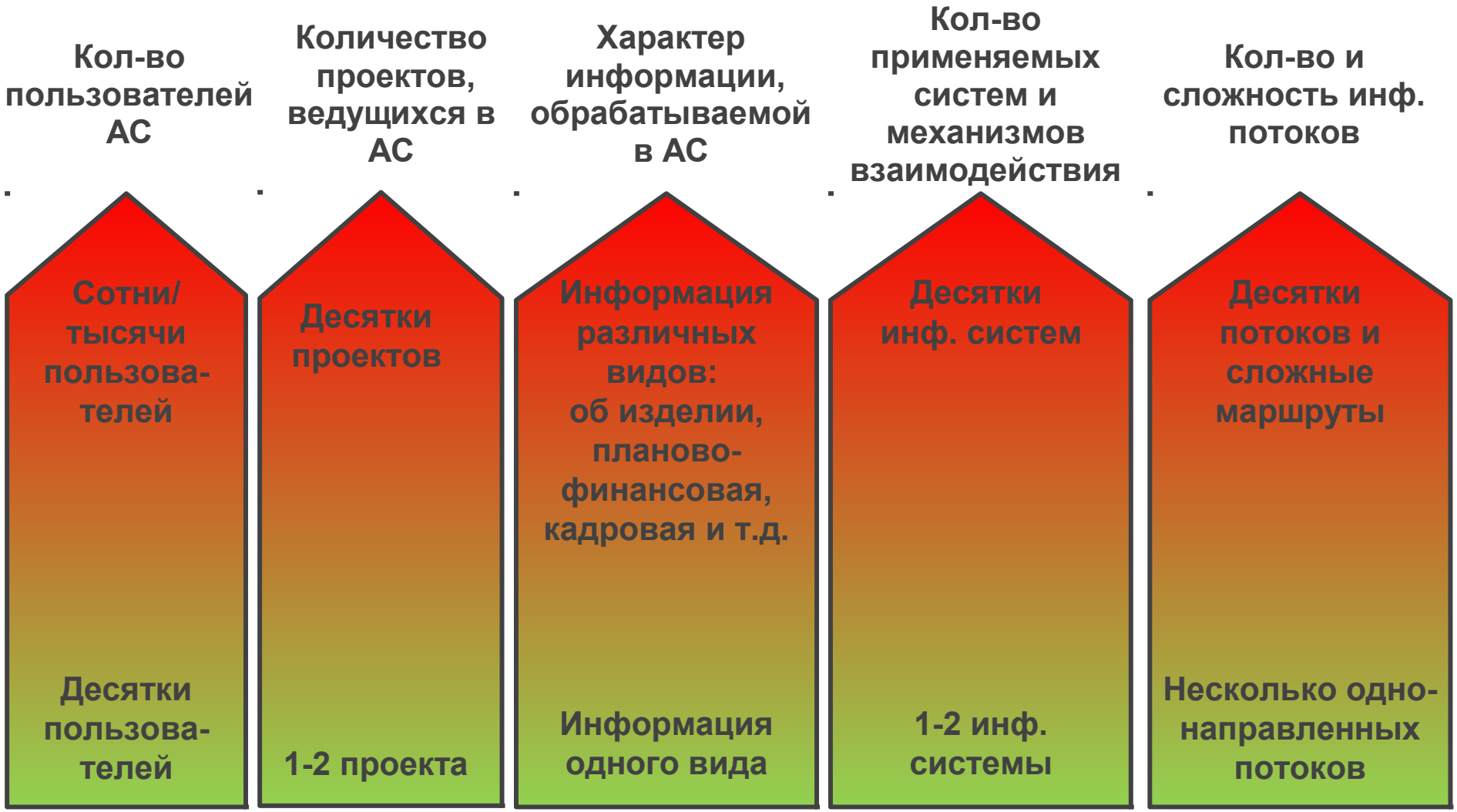
+

Информационные потоки при обработке информации

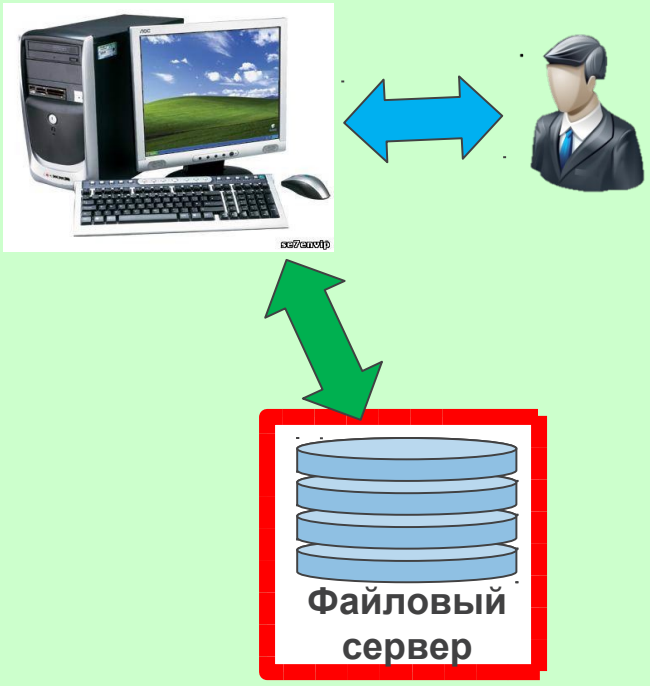


При описании технологии обработки информации мы должны показать, что **все необходимые информационные потоки защищаются** средствами защиты информации, встроенными или наложенными.

Критические изменения при масштабировании автоматизированных систем до уровня подразделения/предприятия



Модель защиты информации при файловом взаимодействии



Поток данных, контролируемый наложенным СрЗИ

В таком режиме работы требования ИБ могут обеспечить **наложенные средства защиты** (например, SecretNet), которые обеспечивают режимы разграничения по требованиям ФСТЭК:

-**Дискреционный** – права доступа к информации каждого субъекта (аналог тематического разграничения);

-**Мандатный** – контролируются потоки информации с разным грифом секретности.

В таком режиме работы можно эффективно автоматизировать работы отдельных специалистов, но **невозможно использовать** современные системы управления данными (PDM, MES, ERP и т.д.), которые используют **клиент-серверную архитектуру**.

Усложнение модели защиты информации при использовании PDM, MES, ERP-систем в АСЗИ

Потоки данных, требующие дополнительного контроля

В клиент-серверной модели:

1.Сервер приложений должен идентифицировать пользователя и определять его допуск к информации;

2.Данные в БД (которая для наложенного СрЗИ является одним файлом) должны быть помечены в зависимости от матрицы доступа;

Вывод:

Обеспечить требования информационной безопасности в такой системе можно только за счет использования **сертифицированных механизмов защиты информации в сервере приложений или СУБД**.

Мандатный метод разграничения доступа – наиболее сложный для реализации в информационной системе

Механизм **мандатного разграничения** доступа – реализуется во исполнение требования ФСТЭК к АСЗИ классов 2А, 1В, 1Б – «**должно осуществляться управление потоками информации с помощью меток конфиденциальности**»

Суть мандатного разграничения доступа:

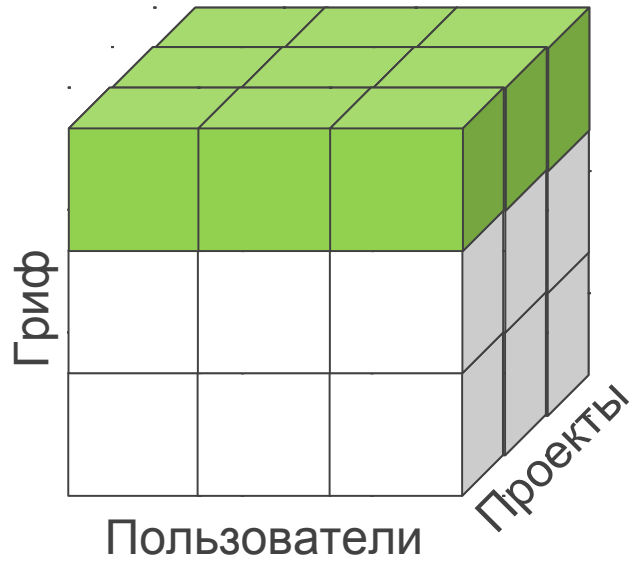
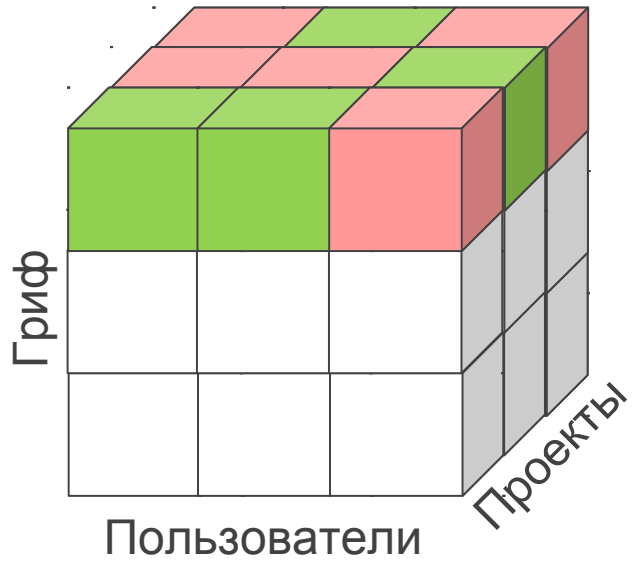
1.При аутентификации в АСЗИ пользователь указывает не только логин, но и **уровень сессии** (фактически уровень грифа), в которой он будет работать с электронными документами

2.Каждый объект (файл) в АСЗИ должен иметь **метку конфиденциальности**.

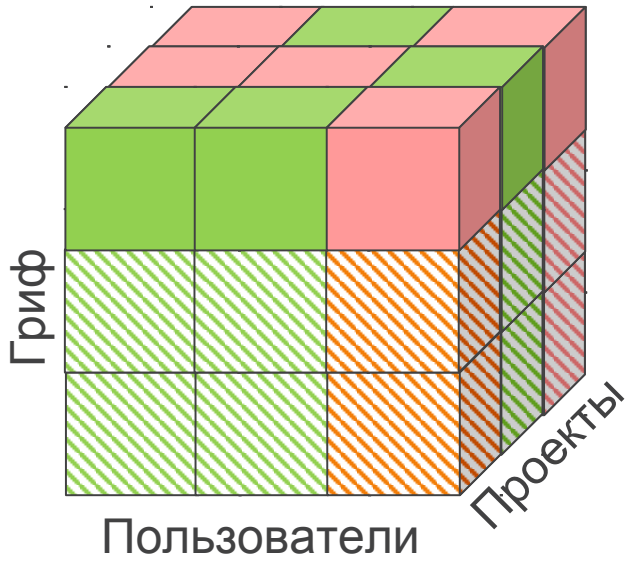
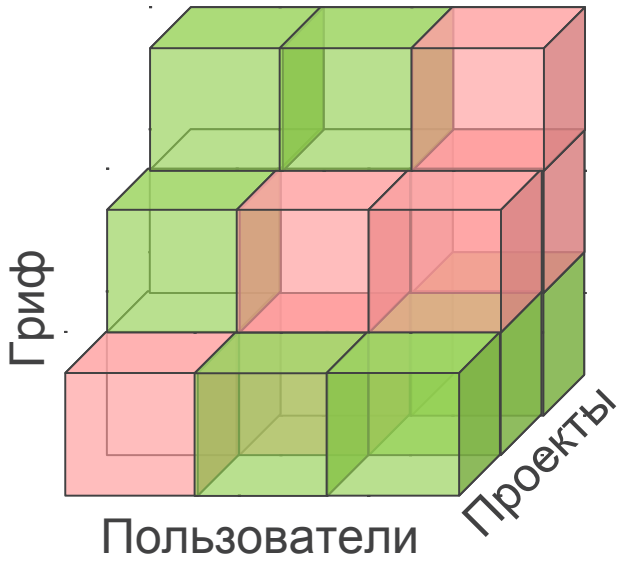
3.При попытке доступа к данным, СрЗИ должно сравнить сессию

Уровень сессии пользователя	Метка конфиденциальности информации		
	ДСП	С	СС
СС	чтение	чтение	чтение и запись
С	чтение	чтение и запись	нет доступа
ДСП	чтение и запись	нет доступа	нет доступа

Отличия в реализации различных вариантов мандатного (МРД) и дискреционного (ДРД) разграничения доступа

Решение на базе зарубежного ПО	Решение на базе ПО АСКОН 2014 года
	
МРД отсутствует - гриф информации максимальный, ДРД отсутствует - все пользователи допущены ко всем данным	МРД отсутствует - гриф информации максимальный, ДРД реализовано - доступ пользователей разграничен по проектам

Отличия в реализации различных вариантов мандатного (МРД) и дискреционного (ДРД) разграничения доступа

Решение на базе ПО АСКОН 2015 года (при условии доработки ПО Лоцман и сертификации на соответствие ТУ)	Перспективное (целевое) мандатное и дискреционное разграничение доступа
	
МРД реализован частично: •для ЭСИ (риф максимальный; •для отдельных документов (риф сохраняется по правилам МРД. Разграничение пользователей по проектам. Технология проектирования только восходящая с ограничениями.	Каждый информационный объект имеет свой гриф, доступ пользователей разграничен по проектам (ДРД) и по форме допуска (МРД). Реализуются восходящая и нисходящая технологии проектирования

Как должно быть сертифицировано ПО для работы с информацией ограниченного распространения

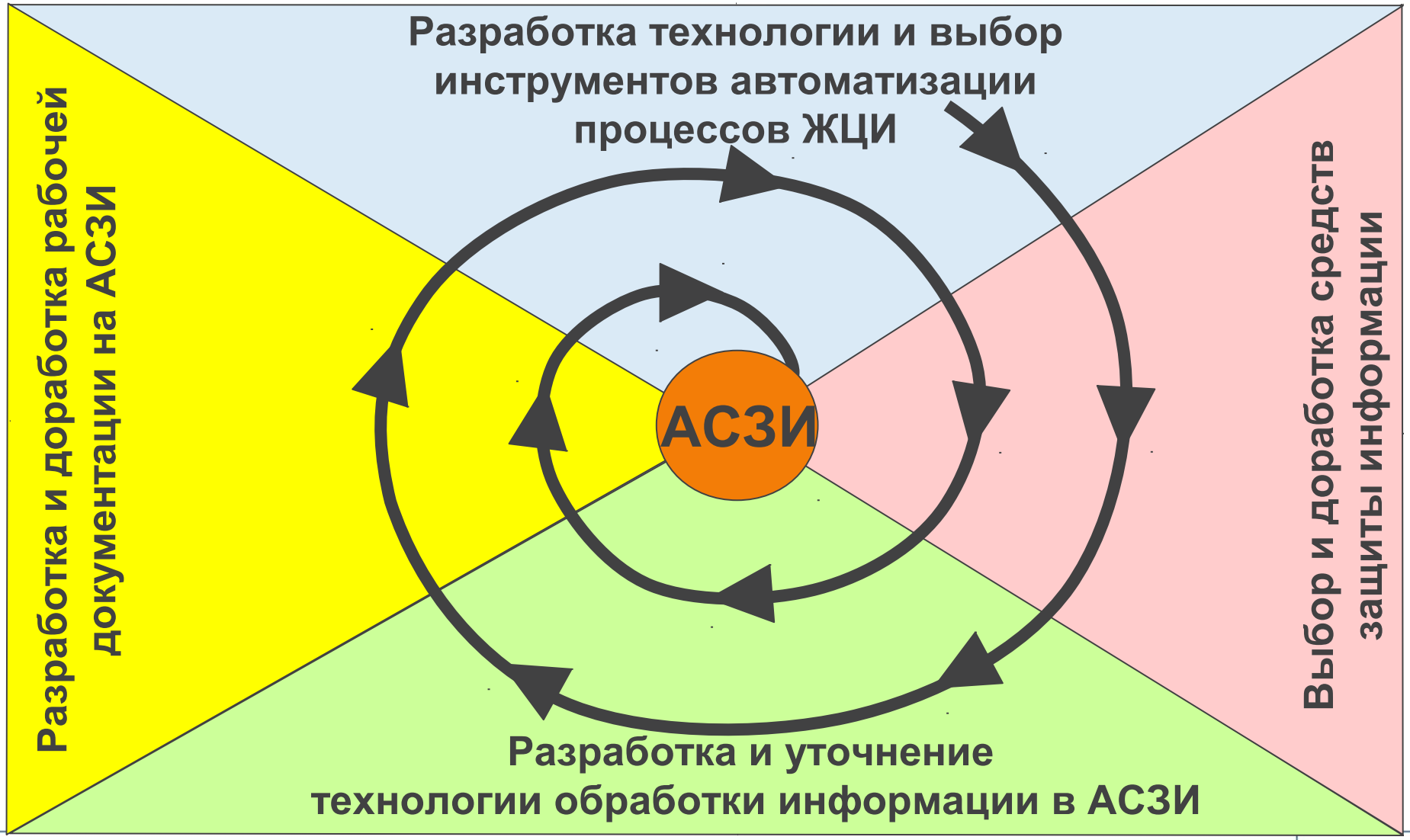
Программное обеспечение, осуществляющее функции защиты информации, должно быть сертифицировано в системе ФСТЭК:

Показатель	АСЗИ для обработки конфиденциальной информации – 1Г	АСЗИ для обработки гостайны – 1Б
Уровень защищенности от несанкционированного доступа к информации (СВТ)	**СВТ 5**	**СВТ 3**
Уровень контроля отсутствия недекларированных возможностей	**НДВ 4**	**НДВ 2**

Сертификация на СВТ (или ТУ) требует не только предоставления исходных кодов ПО, но и собственно реализации механизмов защиты, функционирующих совместимым образом с другими СрЗИ в АСЗИ.

Реализация аналогичных функций в зарубежном ПО (например, MS SQL Server, TeamCenter и т.д.) существует, но поддерживается в отдельных версиях, доступных только разработчикам в военной технике в странах НАТО.

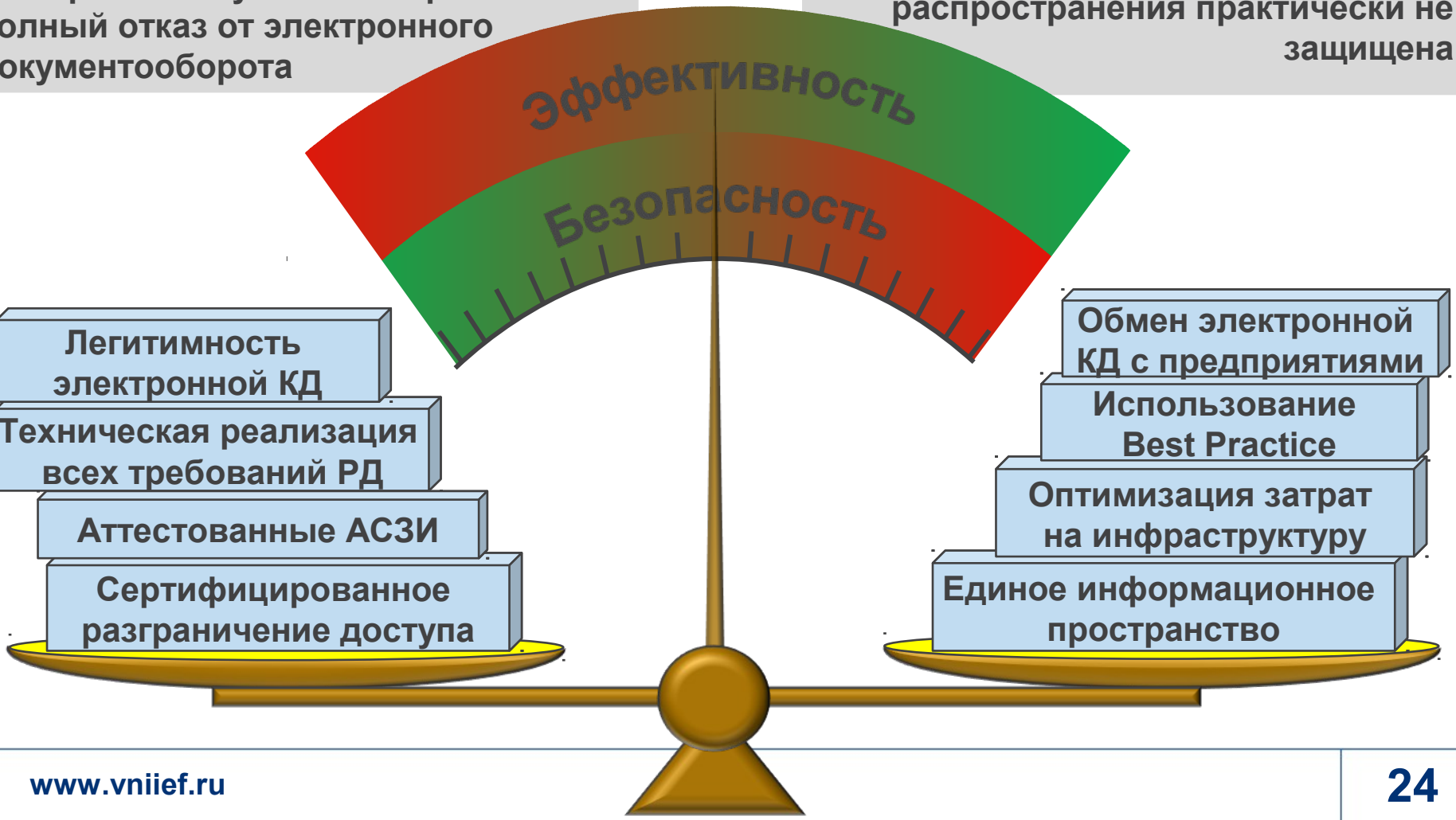
Процесс создания АСЗИ превращается в итерационный путь



Необходим поиск разумного компромисса между требованиями ИБ и эффективностью автоматизации

Полное соблюдение требований ИБ, но использование ПЭВМ в качестве электронного кульмана и фактически полный отказ от электронного документооборота

Самая эффективная автоматизация ЖЦИ, но информация ограниченного распространения практически не защищена



Выводы

1. Информация ограниченного распространения на предприятиях ОПК должна обрабатываться в автоматизированных системах в защищенном исполнении (АСЗИ), аттестованных по требованиям ФСТЭК.

2. Для предприятий ОПК целесообразно строить комплекс (совокупность) АСЗИ двух классов:
   - для обработки несекретной, служебной информации, коммерческой тайны и персональных данных;
   - для обработки и управления информацией на этапах ЖЦИ о проектах/изделиях с максимальным грифом не выше сов.секретно (секретно).

3. Построение на базе АСЗИ единого информационного пространства уровня предприятия требует описания:
   - всех видов информации, планируемой к обработки в АСЗИ – для определения максимальной степени конфиденциальности/секретности;
   - всего ПО (прикладного и системного) и СрЗИ планируемых к использованию – для оценки защиты информационных потоков выбранными средствами защиты.

Выводы

4. Для эффективного использования информационных систем необходимо консолидировано обрабатывать и управлять данными о проектах/планах/изделиях в АСЗИ, соответствующей максимальному уровню конфиденциальности/ секретности данных в проекте;

5. Разграничение доступа (тематическое и по уровню секретности) невозможно реализовать наложенными средствами для информационных систем PDM, ERP, MES, использующих высокопроизводительные промышленные СУБД зарубежного производства;

6. Вопрос вывода из АСЗИ информации на носители различного уровня конфиденциальности/секретности является важнейшим и с самого начала требует внимания проектировщиков АСЗИ;

7. Вопросы информационной безопасности являются ключевыми при создании АСЗИ для обработки информации ограниченного распространения на предприятиях ОПК.