«О практике использования СПО для создания информационных систем Минобороны РФ».

Построение АС ответственного назначения на базе технологий Linux

Метлицкий Юрий Викторович

Содержание

- Основные проблемы обеспечения безопасности информации
- Государственная система защиты информации
- Правовые основы обеспечения защиты информации
- Этапы построения системы защиты информации АС
- Сертификация средств защиты информации
- Экосистема Linux для АС
- Опыт реализации требований ЗИ СВТ от НСД на базе Linux
- Открытый код и контроль отсутствия НДВ
- Выводы

Основные проблемы обеспечения безопасности информации

- ✓ доступность информации
- ✓ конфиденциальность информации
- ✓ достоверность информации
- ✓ целостность информации
- ✓ защита от незаконного тиражирования
- ✓ разграничение ответственности
- ✓ непрерывный контроль над процессами обработки информации

Безопасность АС - это защищенность всех ее компонентов (технических средств, ПО, данных, пользователей и персонала) от нежелательных воздействий.

Государственная система защиты информации

Специальные центры ФСТЭК России

Федеральная служба по техническому и экспортному контролю (ФСТЭК)

Головная научно-исследовательская организация по ЗИ

ФСБ РФ

МВД РФ

МО РФ

СВР РФ

Структурные и межотраслевые подразделения по ЗИ органов государственной власти

Головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские учреждения по защите информации в органах государственной власти

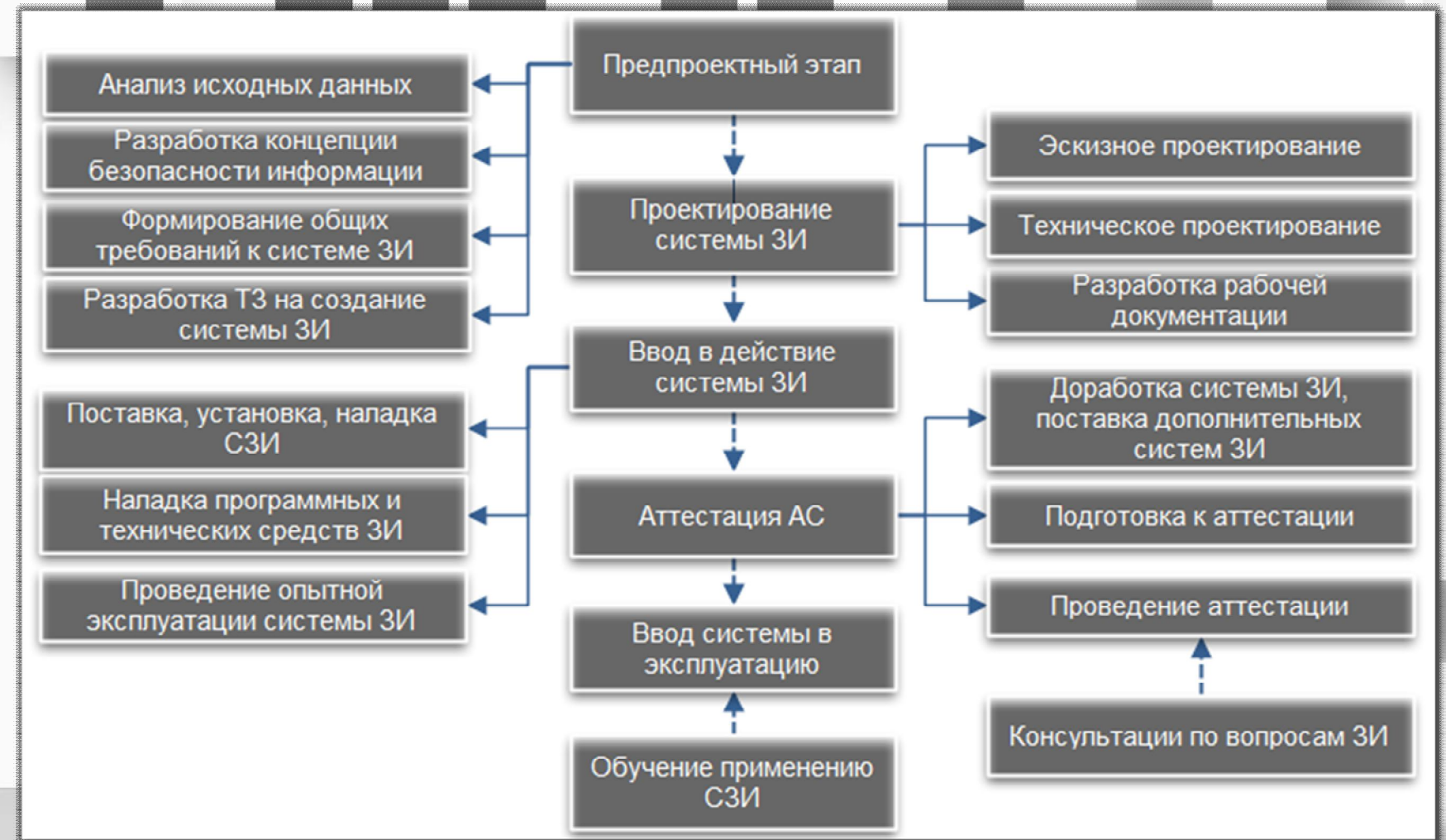
Предприятия, специализирующиеся на проведении работ с использованием сведений, отнесенных к государственной или служебной тайне и их подразделения ЗИ

Правовые основы обеспечения защиты информации

Законы, указы, постановления, стандарты, положения, порядки, РД, другие нормативные и методические документы уполномоченных государственных органов, предусматривают:

- категорирование информации;
- правовой режим ЗИ в отношении сведений, отнесенных к государственной тайне, конфиденциальной информации, персональных данных;
- лицензирование деятельности в области ЗИ;
- аттестация АС на соответствие требованиям ЗИ;
- сертификацию средств ЗИ и средств контроля ЗИ АС;
- создание АС в защищенном исполнении;
- определение прав и обязанностей субъектов в области ЗИ.

Этапы построения системы защиты информации АС



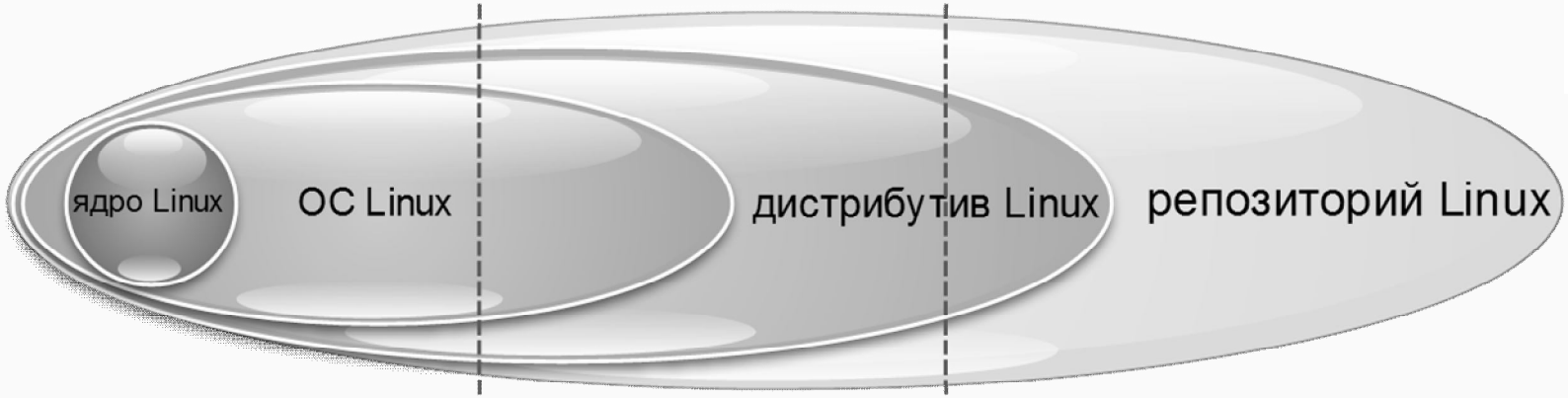
Сертификация средств защиты информации

Сертификация средств ЗИ - деятельность по подтверждению соответствия требованиям государственных стандартов или иных нормативных документов по ЗИ.

Экосистема Linux для АС

ЗАИМСТВОВАНИЕ ДОРАБОТКА ПЕРЕРАБОТКА РАЗРАБОТКА

СВТ ОПО СПО



Опыт реализации требований ЗИ СВТ от НСД на базе Linux

	Требование по ЗИ	Средства Linux	Опыт применения	Компоненты
1	Дискреционный принцип контроля доступа	Подсистема прав UNIX, списки ACL	Полностью заимствована	Ядро, утилиты командной строки
2	Мандатный принцип контроля доступа	Подсистема SELinux	Полностью заменена собственной реализацией модели Белла-ЛаПадула	Ядро, утилиты командной строки, GUI
3	Очистка оперативной памяти	Подсистема управления памятью	Доработана в части многократного затирания ячеек памяти заданной маской	Ядро
4	Очистка внешней памяти	ФС	Разработана для ФС с мандатными механизмами ПРД	Ядро, утилиты командной строки
5	Изоляция модулей	Подсистема управления памятью	Полностью заимствована	Ядро
6	Маркировка документов	Система печати	Доработана в части маркировки документов	Компоненты CUPS

Опыт реализации требований ЗИ СВТ от НСД на базе Linux

	Требование по ЗИ	Средства Linux	Опыт применения	Компоненты
7	Защита ввода и вывода на отчуждаемый физический носитель информации	Подсистема DEVFS, подсистема сетевых сокетов	Доработана в части мандатных механизмов ПРД	ядро
8	Сопоставление пользователя с устройством	Подсистемы обслуживания устройств и ФС (hotlug, mount)	Доработаны в части ведения учтенных отчуждаемых носителей	Средства командной строки
9	Идентификация и аутентификация	Подсистема PAM	Доработана в части назначения мандатных атрибутов ПРД	Средства командной строки
10	Регистрация	Подсистема журналирования ядра и пространства пользователя	Доработана в части регистрации всех указанных требований по ЗИ	Ядро, служба syslog, средства просмотра событий
11	Надежное восстановление	Средства резервного копирования	Доработаны для поддержки мандатного механизма ПРД	Средства Tar, Dump, rsync
12	Целостность КСЗ и контроль модификации	Подсистема контроля целостности	Полностью заимствована	AIDA

Опыт реализации требований ЗИ СВТ от НСД на базе Linux

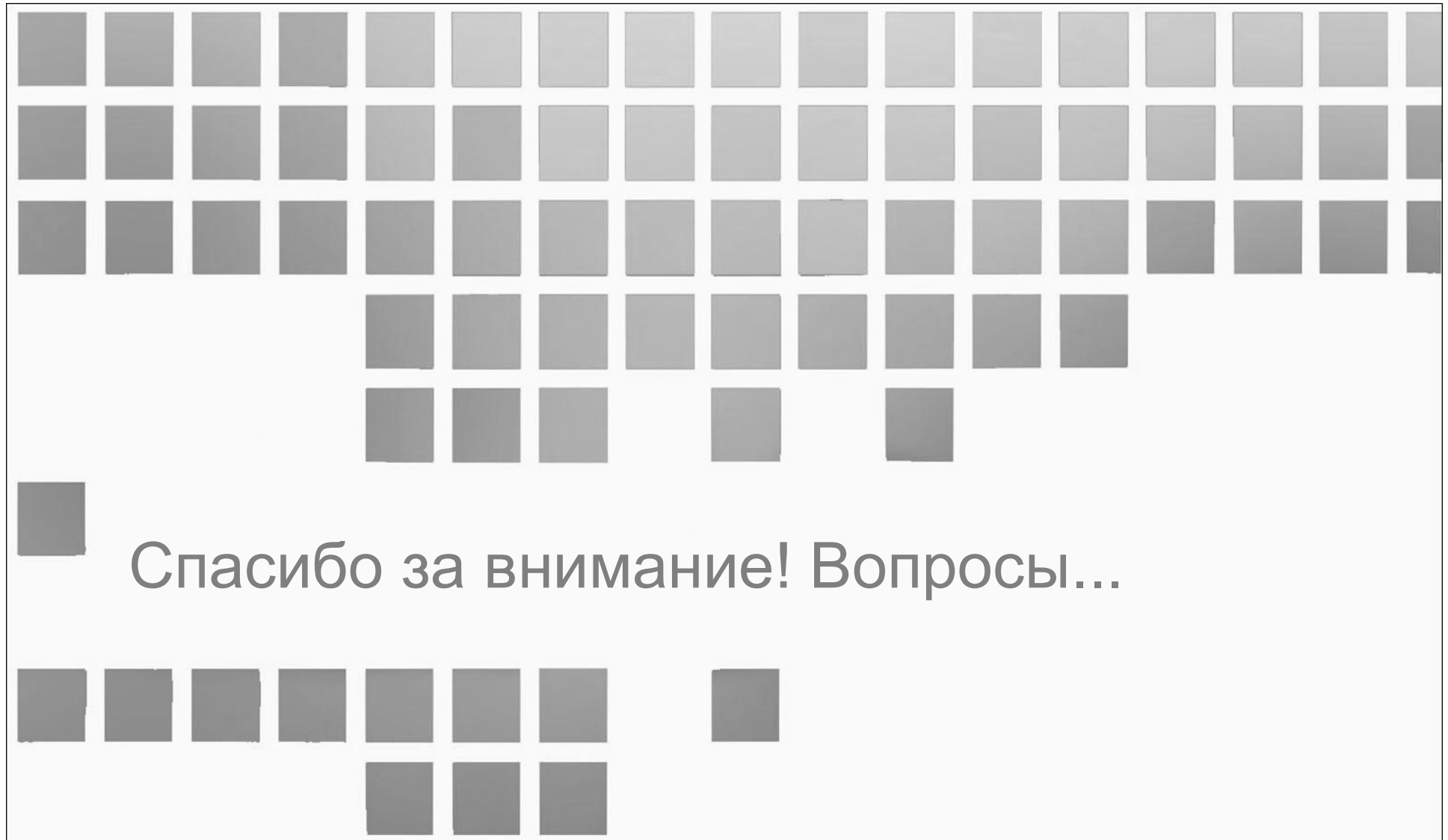
	Требование по ЗИ	Средства Linux	Опыт применения	Компоненты
13	Контроль дистрибуции	Контроль дистрибутивного носителя	Заимствовано решение RedHat и разработана дополнительная процедура	Средства установки
14	Тестирование	Разработан комплект тестов, обеспечивающих проверку функционирования всех подсистем СЗИ		
15	Гарантии проектирования Взаимодействие пользователя с КСЗ Руководство по КСЗ Тестовая документация Конструкторская (проектная) документация	Разработан комплект документов, соответствующих требованиям РД и ГОСТ РФ		

Открытый код и контроль отсутствия НДВ

- Сертификация средств отладки и разработки
- Контроль исходного состояния ПО (воспроизводимость)
- Статический анализ исходных текстов программ
- Динамический анализ исходных текстов программ

Выводы

- СПО является зрелой индустрией
- Открытость обеспечивает возможность анализа и доработки
- На базе СПО можно строить надежные и защищенные решения



Спасибо за внимание! Вопросы...

Метлицкий Юрий
Викторович