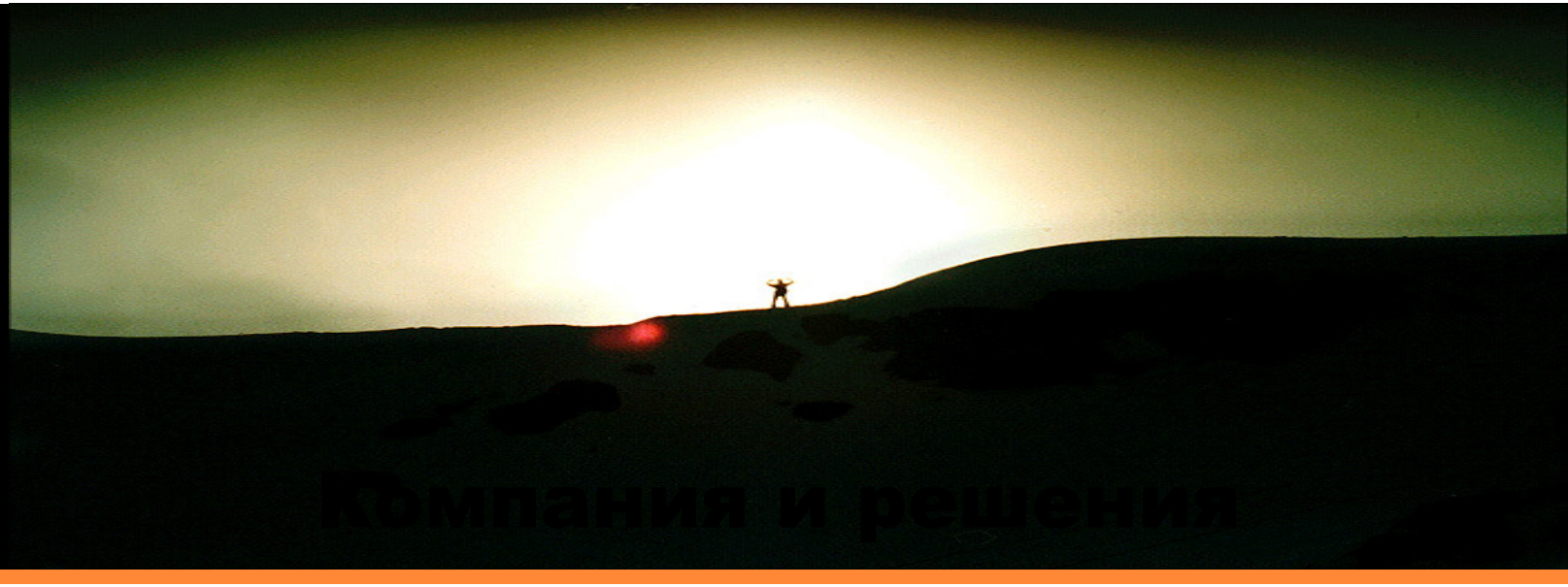
PERIMETRIX



Внедрение решения Perimetrix SafeSpace в ОАО «АВТОВАЗ»

АВТОВАЗ

Информация по проекту

Perimetrix SafeSpace™: Проект на ОАО «АВТОВАЗ»

АВТОВАЗ

1. **Проект внедрения системы «Режима коммерческой тайны ОАО «АВТОВАЗ»» на базе ПО Perimetrix SafeSpace.** Начат в 2012 г.

Цели проекта: Обеспечение прозрачного управления и учета электронных данных, относящихся к коммерческой тайне. Ограничение тех действий пользователей, приложений и процессов в отношении этих данных, которые находящихся вне рамок определенных политик доступа, хранения, обработки и передачи (обмена) данных, относящихся к Коммерческой тайне.

Этап № 1 – Управление конструкторской документацией. Задачи этапа: определение политик обработки, хранения и пересылки (обмена) конструкторских данных (чертежи, спецификации и т.д.) из PLM системы (ЭСКС) и внедрение системы управления этими данными. Этап завершен в 2012 году. В настоящий момент с помощью Perimetrix SafeUse контролируется 2000 именованных пользователей.

Этап № 2 – Управление дизайнерской документацией. Задачи этапа: определение политик обработки, хранения и пересылки (обмена) дизайнерских данных (в форматах CAD, Adobe и других) и внедрение системы управления этими данными. Также, обеспечение безопасной передачи между бюро в Москве и Тольятти, с учетом преемственности политик. Этап начат в конце 2012 и завершен в начале 2013 года. Perimetrix SafeUse - 200 именованных пользователей.

Этап № 3 – Управление информацией Системы контроля качества. Задачи этапа: определение политик обработки, хранения и пересылки (обмена) данных Системы контроля качества и внедрение системы управления этими данными. Начат в начале 2014 г. Плановое окончание – второе полугодие 2014 года. Perimetrix SafeUse – 1200 именованных пользователей.

Также, в 2014 – 15 годах планируется:

Этап № 4 – Управление информацией из Системы подготовки документов правления ОАО «АВТОВАЗ» - 100 именованных пользователей SafeUse

Этап № 5 – Управление информацией из Системы «Лоцман» (Строительная документация) – 300 именованных пользователей Perimetrix SafeUse

2. **Проект внедрения системы «Защиты персональных данных ОАО «АВТОВАЗ»» на базе ПО Perimetrix SafeSpace** - 3200 пользователей

Perimetrix SafeSpace™: Проект на ОАО «АВТОВАЗ»

АВТОВАЗ

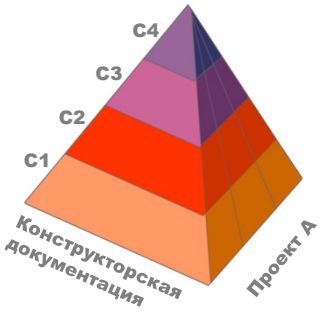
Данная презентация охватывает завершенные этапы проекта: Этап 1 «Управление конструкторской документацией» (КД) и Этап 2 «Управление дизайнерской документацией» (ДД)

Первоначально, причиной для внедрения системы «Режима коммерческой тайны» послужило:

1. **Требование акционера Renault – Nissan по обеспечению надежной защиты информационных активов, в части передаваемой технической документации;**
2. **Появление на рынке большого количества некачественных запчастей, выпущенных, неавторизованными производителями, возможно по технической документации АВТОВАЗ, но из низкокачественных материалов и без оплаты роялти владельцу интеллектуальной собственности.**

Далее, в проект были включены и другие информационные активы, составляющие коммерческую тайну

Основные этапы внедрения



В рамках внедрения Этапов 1 и 2 были проведены:

- **Выявление объектов защиты и составление классификатора данных, составляющих коммерческую тайну;**
- **Разработка модели угроз утечки классифицированных данных (далее КД);**
- **Разработка политик и процедур в части обработки, хранения и передачи (обмена) КД;**
- **Моделирование новых \ Корректирование бизнес – процессов и процедур, в части работы с КД;**
- **Инсталляция, настройка и развертывание ПО Perimetrix;**
- **Опытная эксплуатация системы «Режима коммерческой тайны»;**
- **Перевод системы в промышленную эксплуатацию**

Разработка политик «Режима коммерческой тайны» (РКТ)

В общем виде политика Режима коммерческой тайны может быть описана следующими основными положениями:

1. Вся защищаемая информация должна быть классифицирована в соответствии с определенной схемой. Схема классификации должна быть разработана таким образом, чтобы обеспечить достаточную гранулярность назначения полномочий субъектам. Как минимум, информация должна классифицироваться по шкале секретности в сочетании со шкалой, отражающей смысловую (функциональную) составляющую информации.

2. Для каждой категории информации необходимо определить следующие параметры:
a) список рабочих станций, на которых возможна обработка информации;
b) список пользователей (учетных записей), имеющих допуск к обработке информации;
c) список допустимых для обработки приложений;
d) список допустимых для хранения файловых форматов;
e) список допустимых мест хранения информации, в том числе и серверных (сетевые папки, СУБД и прочее);
f) список разрешенных к использованию периферийных устройств;
g) список разрешенных для печати принтеров;
h) схемы бизнес-процессов обработки данных с учетом разрешенных мест хранения, используемых приложений
i) процедуры раскрытия защищаемых данных третьим лицам

Политики РКТ в части конструкторской и дизайнерской документации

В рамках защиты КД и ДД политика безопасности сформулирована следующим образом:

СУТЬ ПОЛИТИКИ: Конструкторские данные могут храниться только на сервере ЭСКС (PLM система) и жестких дисках авторизованных компьютеров. Дизайнерские данные могут храниться только на файловых серверах Бюро по дизайну в Москве и Тольятти. Обработка КД и ДД возможна только с использованием определенных политиками приложений. Запрещается копирование КД и ДД на съемные накопители, сетевые папки, передача по электронной почте, передача в интернет, кроме определенных политиками случаев. Порядок отступления от данных правил и методики раскрытия информации третьим лицам строго регламентированы.

Более подробно политика описывается следующими положениями:

1. ДД и КД может обрабатываться только на рабочих станциях, защищенных агентом Perimetrix SafeUse и только пользователями с надлежащим допуском;
2. ДД и КД может обрабатываться только приложениями, определенными политиками;
3. ДД и КД может храниться только в местах хранения, определенных политиками;
4. Допустимыми для хранения форматами файлов являются только форматы, определенные политиками;
5. Допустимыми для печати являются только авторизованные политиками принтеры;
6. Раскрытие защищаемой ДД и КД третьим лицам производится в следующих случаях:

a) Передача ДД и КД поставщикам, имеющим соглашение о неразглашении конфиденциальной информации с ОАО “АВТОВАЗ” через веб-портал “Windchill/Project Link”.

7. Специальные процедуры.

a) Для обмена ДД и КД с пользователями, защищенными агентом Perimetrix SafeUse, используется специальная процедура упаковки данных в криптоконтейнер Perimetrix SafeStore. После помещения информации в криптоконтейнер ее можно посылать по электронной почте, копировать на съемные диски, передавать в интернет и т.д. Агент не накладывает ограничений на перемещение криптоконтейнера, однако извлечь данные из криптоконтейнера для последующей работы с ними возможно только на рабочей станции, защищенной агентом Perimetrix SafeUse.

b) Для перемещения, переименования, удаления ДД и КД, находящихся на жестком диске защищаемой станции, предусмотрены специальные, определенные политиками процедуры.

Схема работы системы Режима КТ в части КД и ДД (рисунок)

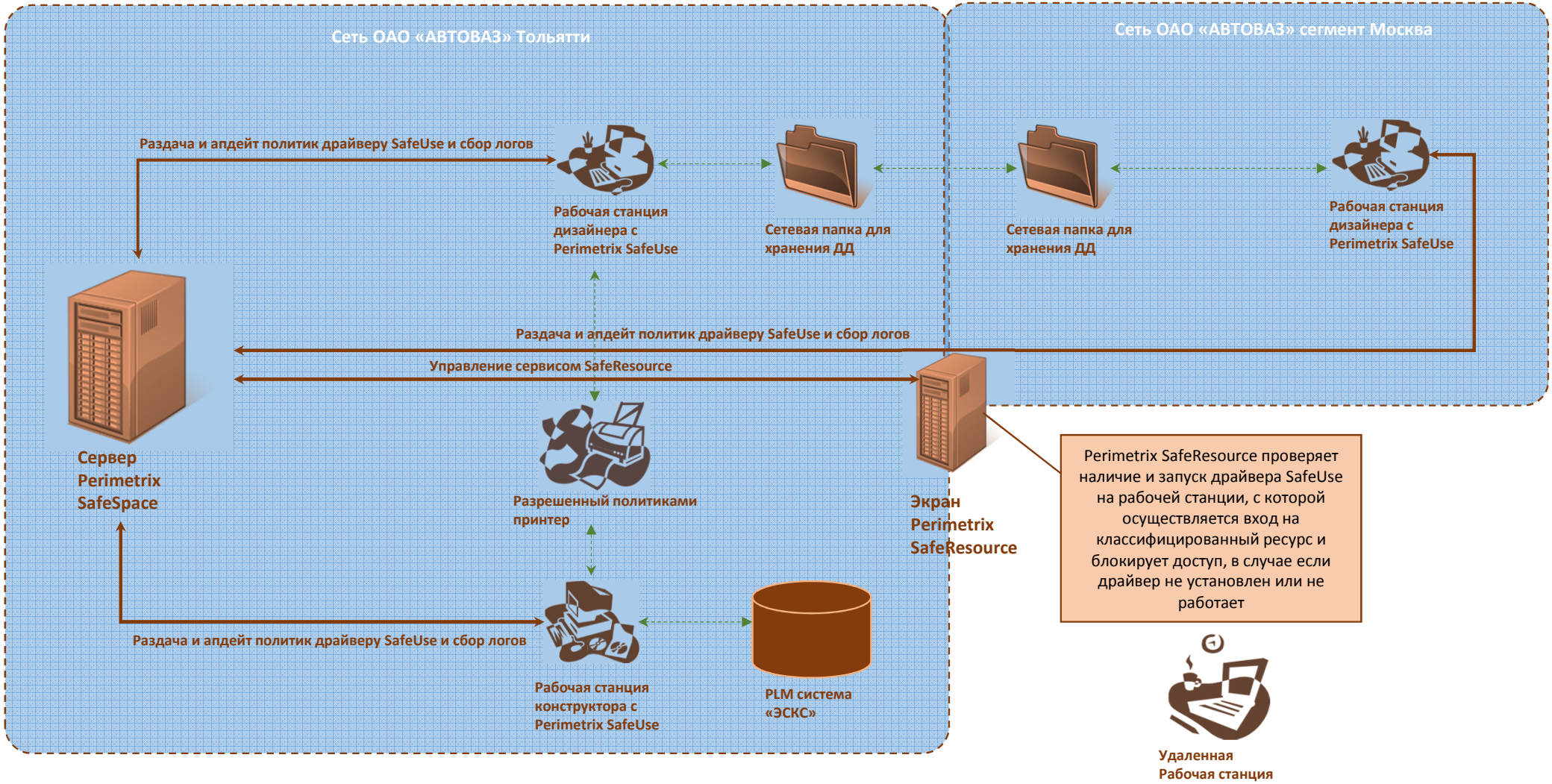


Схема работы системы Режима КТ в части КД и ДД

Perimetrix SafeSpace контролирует доступ пользователей, приложений, процессов, устройств к классифицированной информации таким образом, что пользователь может делать с защищаемыми данными только то, что разрешено политиками Режима КТ, которые, в свою очередь связаны с бизнес – процессом.

Пользователь может:

- **Сохранять классифицированные данные в разрешенном политиками месте и разрешенном формате (КД – ЭСКС и жесткий диск, ДД – на выделенных сетевых папках в разрешенных форматах);**
- **Обрабатывать классифицированные данные только определенными политиками приложениями;**
- **Печатать только на определенный политиками принтер;**
- **Передавать и пересылать классифицированные данные только определенным политиками образом (через портал, или упаковав в криптоконтейнер)**

Любые другие, не разрешенные политиками действия пользователя, в отношении классифицированной информации, блокируются.

Perimetrix SafeSpace собирает и хранит лог – информацию о действиях в отношении классифицированной информации для целей отёчности и анализа.

Техническая реализация системы режима КТ

Рабочая станция Администратора Perimetrix SafeSpace – Internet browser

«ТОНКИЙ КЛИЕНТ»

Сервер PerimetrixSafeSpace
HP ProLiant DL580G7

Architecture:	x86_64
CPU(s):	Xeon 4x8
CPU MHz:	1064.0
Memory:	256 GB
HDD1 (OS + SafeSpace)	1TB
HDD2 – (Oracle NAS), 1 TB	

OS: Red Hat Enterprise Linux Server release 6.3 (Santiago)

Database: ORACLE 11g

TCP/IP

2200 рабочих станций под управлением Windows XP, Vista, Windows 7

Рабочая станция дизайнера с Perimetrix SafeUse

Рабочая станция дизайнера с Perimetrix SafeUse

Спасибо за внимание!

Компания Perimetrix

Россия и СНГ : **ООО «ПЕРИМЕТРИКС»** 119607, Москва, Мичуринский проспект, д. 45
Телефон: +7 495 737 99 91; Факс: +7 495 737 99 92

Южно – Африканская Республика: **Perimetrix SA (Pty) Ltd** Balblair Building, Kildrummy Office Park,Cnr Witkoppen Road and Umhlanga Drive,
Paulshof, 2056
Tel: +27 11 319 7206; Fax: +27 86 669 7800