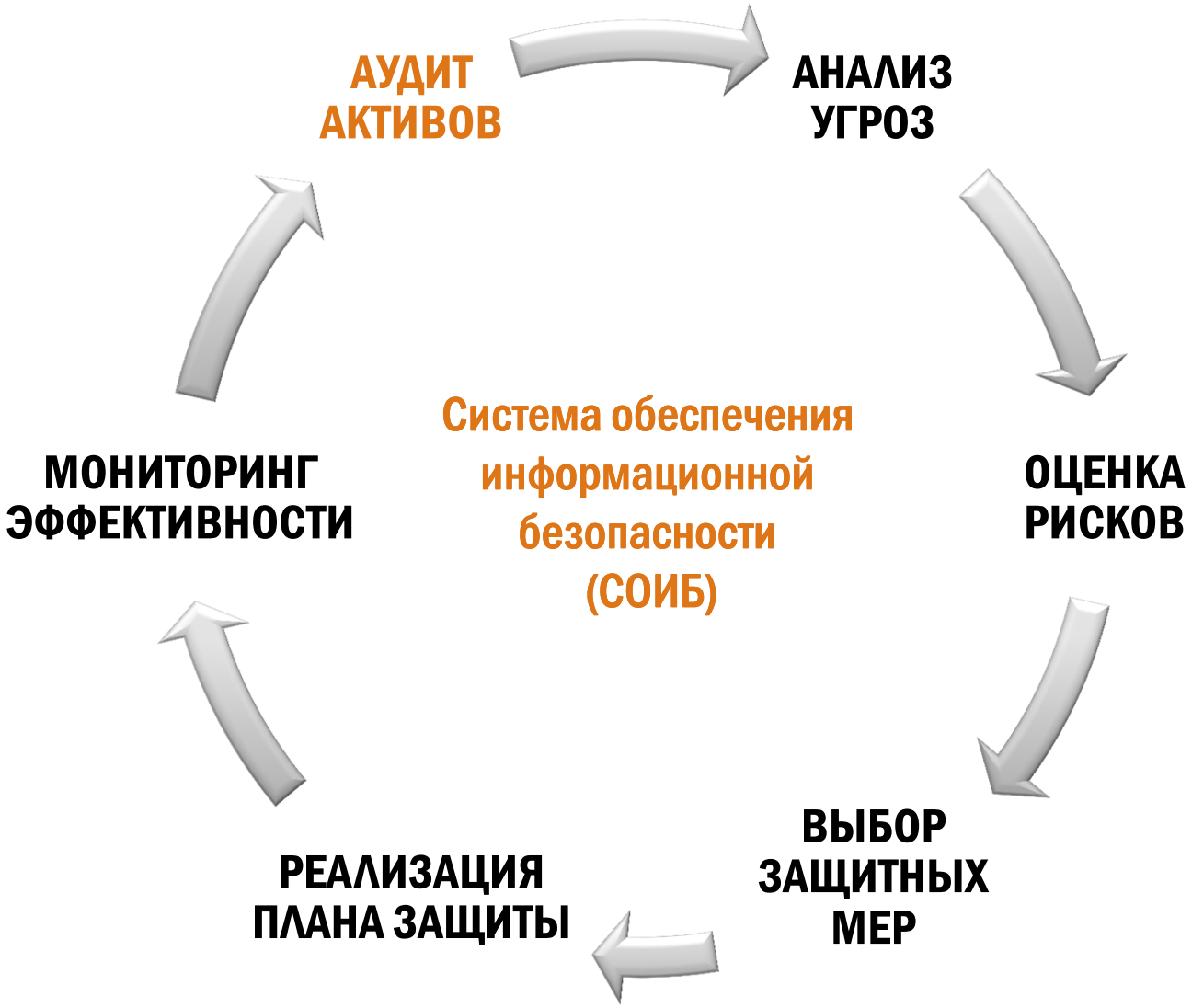
ТЕХНИЧЕСКИЕ СРЕДСТВА РЕАЛИЗАЦИИ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

ПОДХОД И РЕШЕНИЯ КОМПАНИИ PERIMETRIX

НЕПРЕРЫВНЫЙ ЦИКЛ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ



СОСТАВ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3

АУДИТ И МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Управление инцидентами, управление паролями, контроль работы пользователей, администраторов ИТ, …

2

УПРАВЛЕНИЕ ДОСТУПОМ И ЗАЩИТА ИНФОРМАЦИИ
Разграничение доступа, шифрование данных, электронные ключи и подписи, защита от утечек, …

1

«САНИТАРИЯ И ГИГИЕНА» ИТ-СРЕДЫ
Антивирусы, резервное копирование, обновления ПО, шлюзы безопасности, …

ПРАВОВОЕ ПОЛЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РЕГУЛИРУЮЩИЕ ОРГАНЫ

Федеральная служба безопасности (ФСБ),
Федеральная служба по техническому и экспортному контролю (ФСТЭК),
Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор),
Центральный банк Российской Федерации (ЦБРФ)
…

НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

98 ФЗ «О коммерческой тайне»
152 ФЗ «О персональных данных»
…

СТАНДАРТЫ

ГОСТы 50992, 13335, 15408, ISO 27001
Стандарт Банка России
…

СТРУКТУРА СИСТЕМЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ

СИСТЕМА ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ

- **ПРАВОВЫЕ МЕРЫ**
- **ОРГАНИЗАЦИОННЫЕ МЕРЫ**
- **ТЕХНИЧЕСКИЕ МЕРЫ**

Задача **правовых мер** – создание юридических предпосылок для последующего возмещения ущерба (в случае реализации угрозы утечки информации)

Организационные меры предназначены для минимизации риска нарушения конфиденциальности информации путем

- повышения уровня культуры при работе с КТ
- создания нормативной базы для управления КТ
- создания предпосылок для эффективного управления системой зашиты.

Технические меры направлены на

- **предотвращение возможности утечки** информации, содержащей КТ
- **своевременное обнаружение** фактов нарушения режима КТ

ОЖИДАНИЯ РУКОВОДСТВА ОТ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

НАДЕЖДЫ:

- Воспрепятствует краже информации, ее обесцениванию путем разглашения
- Наведет порядок при работе с ценной информацией
- Повысит персональную ответственность сотрудников и руководителей за сохранность ценность информации на предприятии
- Позволит в судебном порядке взыскивать с виновных ущерб от утечки информации

СТРАХИ:

- Может мешать рабочим процессам, критично сказываться на производительности
- Потребует от сотрудников дополнительных затрат времени на бюрократические процедуры
- Негативно повлияет на атмосферу в коллективе, снизит мотивацию к труду
- Потребует увеличения численности служб безопасности и иных затрат на помещения, оборудование, ПО и др. технические меры
- При неправильной реализации не защитит ценную информацию, затруднит использование «простой» информации

РАЗУМНАЯ РЕАЛИЗАЦИЯ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

- ✓ Привлечение владельца данных к принятию решения о ценности информации и степени конфиденциальности, к ее категоризации
- ✓ Четкие критерии для определения конфиденциальной информации, сокращение перечня информации, относящейся к КТ
- ✓ Формализация понятия коммерческой тайны, стандартизация содержащих ее документов и по возможности упрощение связанных с ней бизнес-процессов
- ✓ Дробление объектов, содержащих КТ, для снижения рисков
- ✓ Минимизация негативного влияния на основную производственную деятельность
- ✓ Обеспечение работоспособности режима КТ при взаимодействии в группе компаний, с контрагентами
- ✓ Создание KPI, мотивирующих сотрудников на соблюдение режима КТ
- ✓ KPI специалистов блока безопасности основан на **предотвращении** действий с КТ, не предусмотренных режимом, а не на фиксировании утечек

«ЖИЗНЕННЫЙ ЦИКЛ» РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

1 ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ ЗАЩИТЫ

- Коммерческая тайна;
- Персональные данные;
- Информация для регуляторов.

2 АНАЛИЗ РИСКОВ

- Выявление областей рисков, содержащих коммерческую тайну;
- Оценка рисков разглашения коммерческой тайны;
- Выявление наиболее критичных рисков.

3 РАЗРАБОТКА КЛАССИФИКАТОРА

- Выявление наиболее критичной для разглашения коммерческой тайны;
- Разработка классификатора коммерческой тайны;
- Разработка политик, сопровождающих классификатор.

4 ВЫРАБОТКА ТРЕБОВАНИЙ

Области требований:

- Законы и нормативные акты;
- Организационные меры (политики, процедуры, роли);
- Технические меры;
- Аудит;
- Персонал и компания.

5 РЕАЛИЗАЦИЯ РЕЖИМА

- Выполнение организационных мероприятий (приказы, инструкции);
- Внедрение и настройка технических средств;
- Реализация режима и политик на местах.

БАЗОВЫЕ ШАГИ ПО РЕАЛИЗАЦИИ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

1 КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2 ОПРЕДЕЛЕНИЕ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ

3 РАЗРАБОТКА ПОЛИТИК РАБОТЫ С ИНФОРМАЦИЕЙ

4 ВНЕДРЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИЕЙ

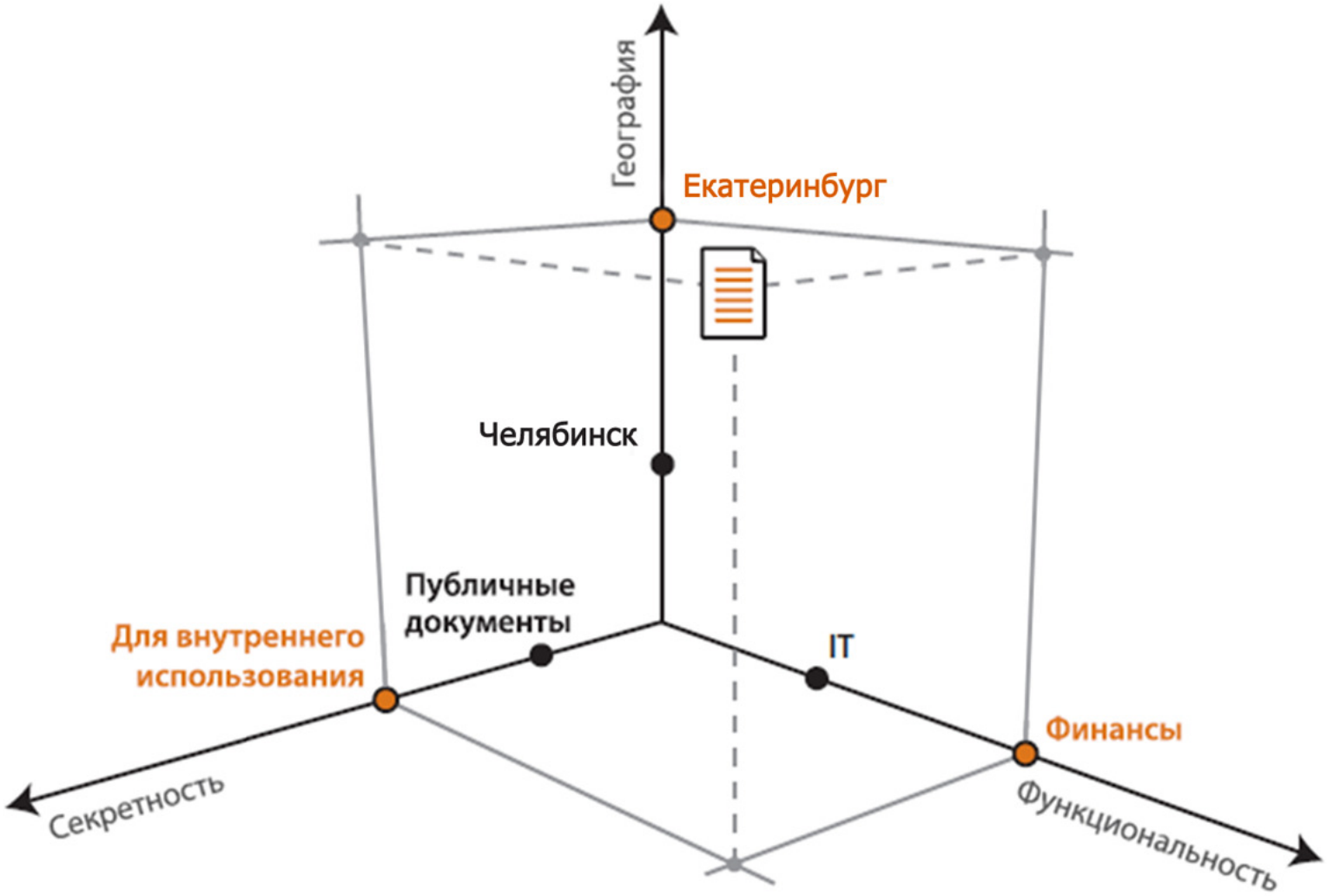
КЛАССИФИКАЦИЯ: МНОГОМЕРНАЯ МОДЕЛЬ КАТЕГОРИЙ

СЕКРЕТНОСТЬ

ФУНКЦИОНАЛЬНОСТЬ

ГЕОГРАФИЯ

КЛАССИФИКАЦИЯ: ДАННЫЕ В МНОГОМЕРНОЙ МОДЕЛИ



БАЗОВЫЕ ШАГИ ПО РЕАЛИЗАЦИИ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

1 КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2 ОПРЕДЕЛЕНИЕ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ

3 РАЗРАБОТКА ПОЛИТИК РАБОТЫ С ИНФОРМАЦИЕЙ

4 ВНЕДРЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИЕЙ

КЛАССИФИКАЦИЯ: ПОЛНОМОЧИЯ ПОЛЬЗОВАТЕЛЕЙ

	Сотрудник центрального департамента финансов	Руководитель филиала в Екатеринбурге
СЕКРЕТНОСТЬ	ДЛЯ ВНУТРЕННЕГО ПОЛЬЗОВАНИЯ	СТРОГО КОНФИДЕНЦИАЛЬНО
ФУНКЦИОНАЛЬНОСТЬ	ФИНАНСЫ	*
ГЕОГРАФИЯ	РОССИЯ	ЕКАТЕРИНБУРГ

БАЗОВЫЕ ШАГИ ПО РЕАЛИЗАЦИИ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

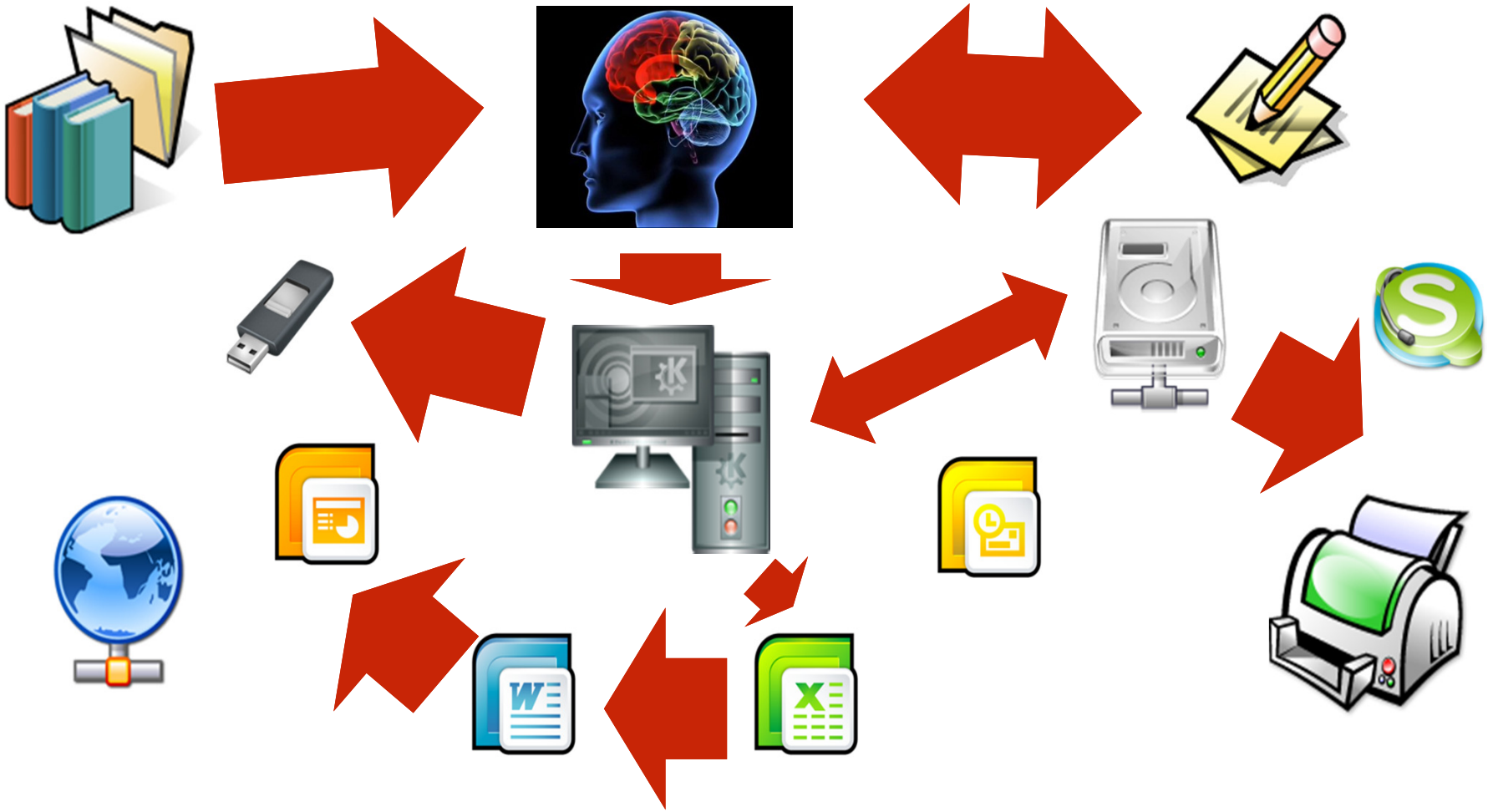
1 КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

2 ОПРЕДЕЛЕНИЕ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ

3 РАЗРАБОТКА ПОЛИТИК РАБОТЫ С ИНФОРМАЦИЕЙ

4 ВНЕДРЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИЕЙ

АНАТОМИЯ УТЕЧКИ



РЕЖИМ КТ – ТИПОВЫЕ ПАРАМЕТРЫ НИЗКОУРОВНЕВЫХ ПОЛИТИК

Необходимо определить следующие параметры:

- список рабочих станций, на которых возможна обработка информации;
- список пользователей (учетных записей), имеющих допуск к обработке информации;
- список допустимых для обработки приложений;
- список допустимых для хранения файловых форматов;
- список допустимых мест хранения информации, в том числе и серверных (сетевые папки, СУБД и прочее);
- список разрешенных к использованию периферийных устройств;
- список разрешенных для печати принтеров;
- схемы бизнес-процессов обработки данных с учетом разрешенных мест хранения, используемых приложений;
- процедуры раскрытия защищаемых данных третьим лицам.

ОСНОВНОЙ ПРИНЦИП ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ЗАПРЕЩЕНО ВСЕ,
КРОМЕ ТОГО,
ЧТО В ЯВНОМ ВИДЕ
РАЗРЕШЕНО

БАЗОВЫЕ ШАГИ ПО РЕАЛИЗАЦИИ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

1 КЛАССИФИКАЦИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

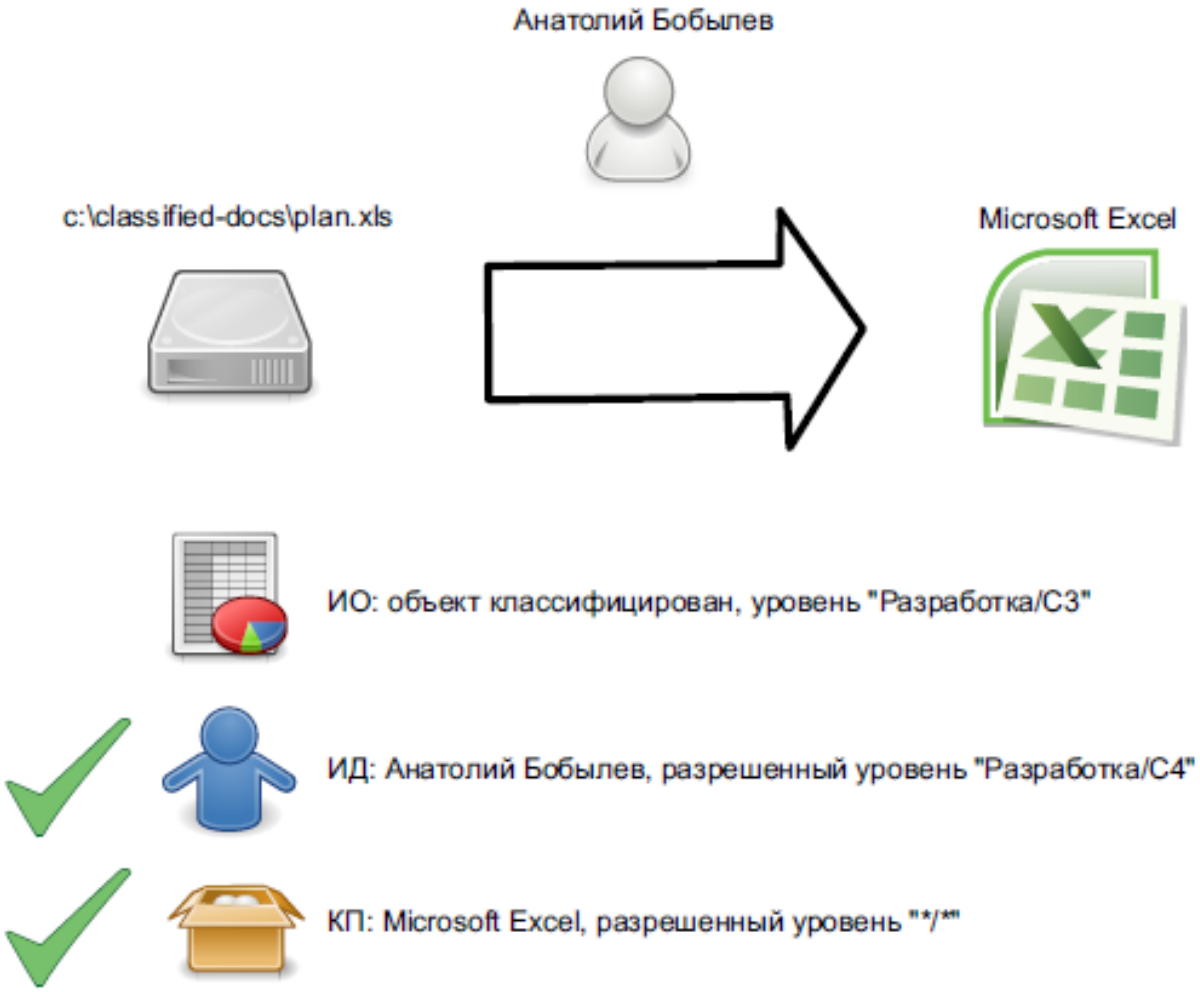
2 ОПРЕДЕЛЕНИЕ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ

3 РАЗРАБОТКА ПОЛИТИК РАБОТЫ С ИНФОРМАЦИЕЙ

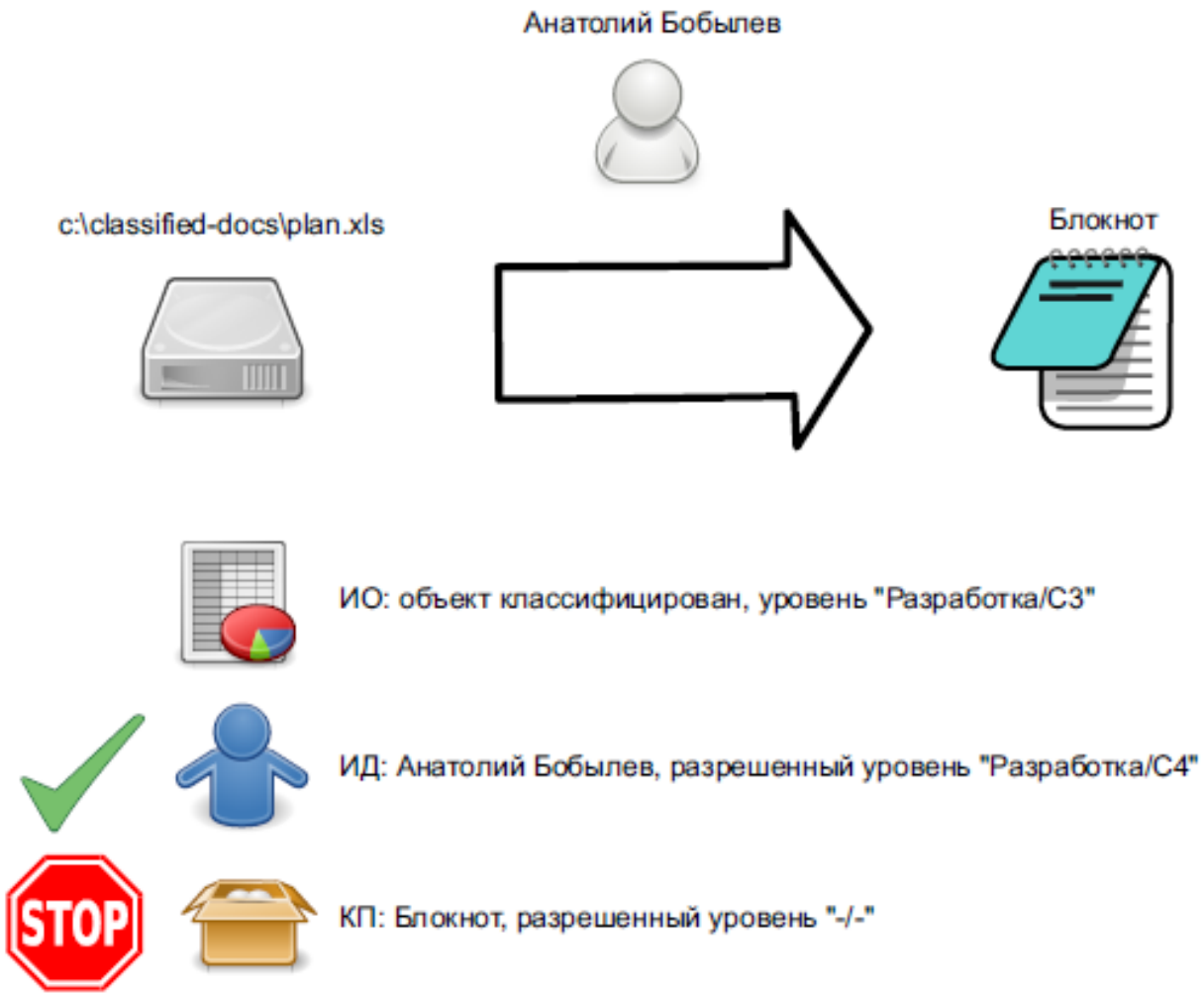
4 ВНЕДРЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КЛАССИФИЦИРОВАННОЙ ИНФОРМАЦИЕЙ

УНИВЕРСАЛЬНАЯ МОДЕЛЬ СОБЫТИЙ И ЛОГИКА ПРИНЯТИЯ РЕШЕНИЙ

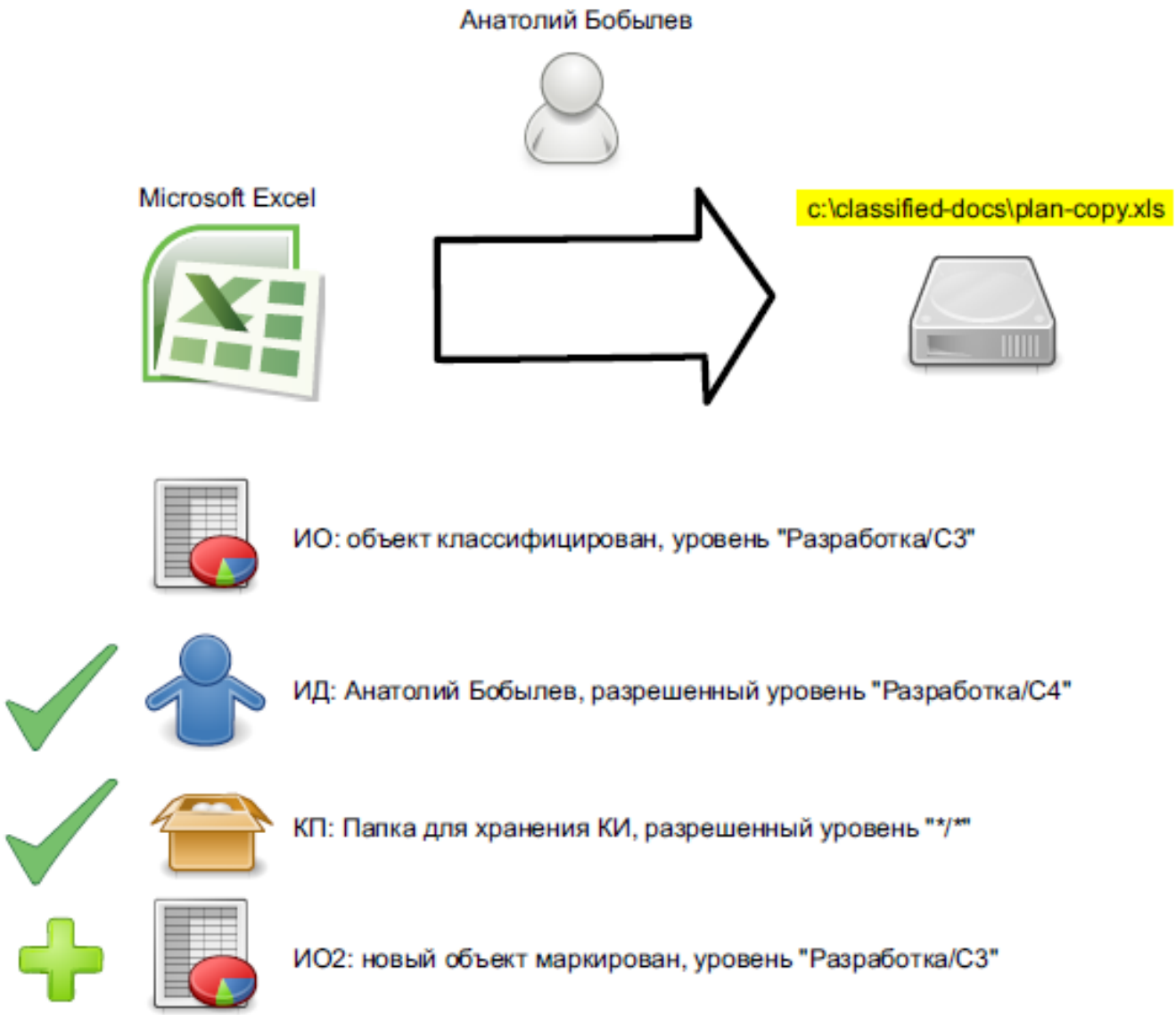
РАЗРЕШЕННОЕ ДЕЙСТВИЕ С КЛАССИФИЦИРОВАННЫМ ОБЪЕКТОМ



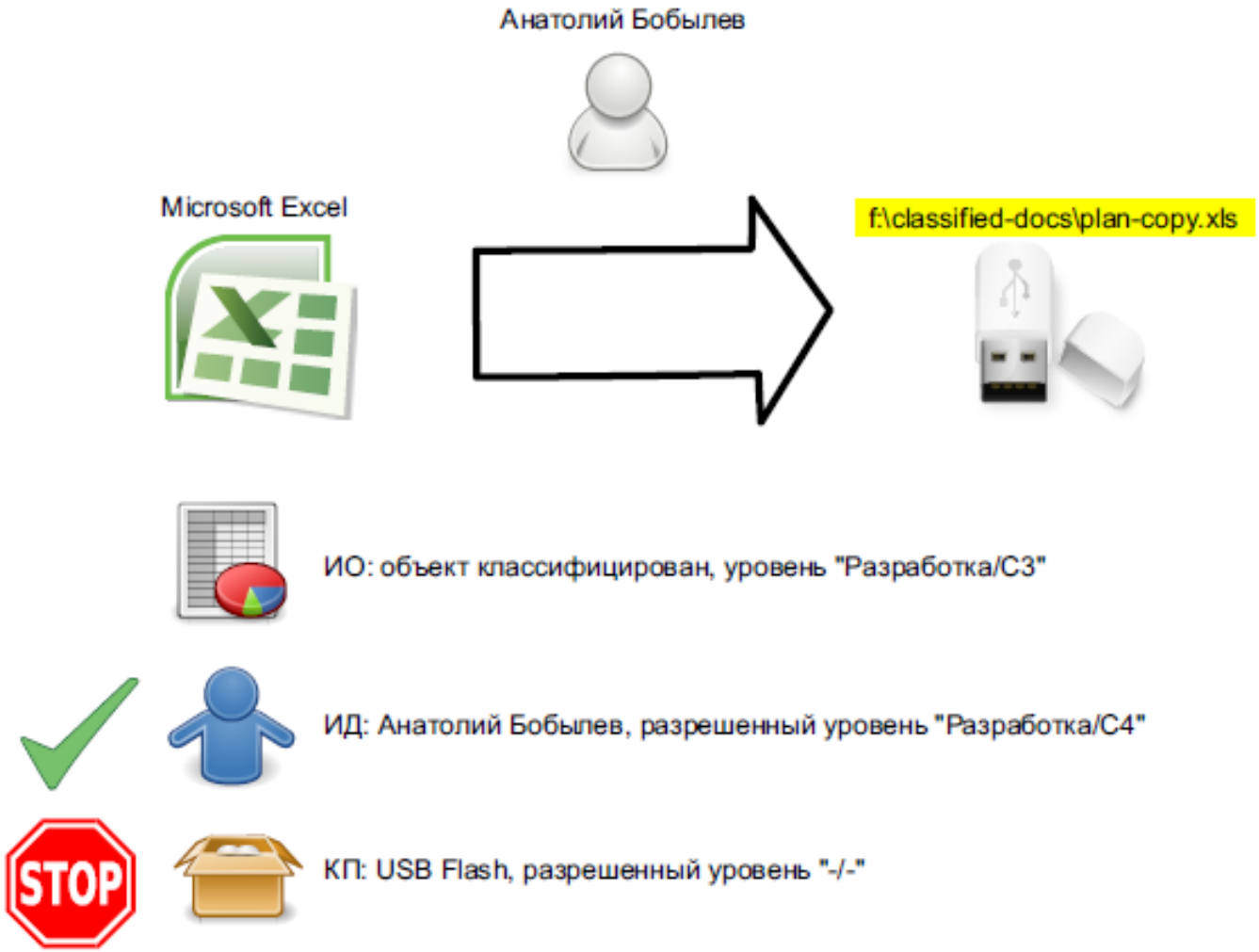
НЕРАЗРЕШЕННОЕ ДЕЙСТВИЕ С КЛАССИФИЦИРОВАННЫМ ОБЪЕКТОМ



МАРКИРОВКА ПРОИЗВОДНОГО ФАЙЛА



НЕДОПУСТИМОЕ МЕСТО ХРАНЕНИЯ



РАЗРЕШЕННОЕ ДЕЙСТВИЕ С КЛАССИФИЦИРОВАННЫМ ОБЪЕКТОМ

Анатолий Бобылев

```
MAIL FROM:<anatoli.bobylev@perimetrix.com>
RCPT TO:<andrey.tatarenko@perimetrix.com>
DATA
From: Anatoli Bobylev <anatoli.bobylev@perimetrix.com>
To: Andrey Tatarenko <andrey.tatarenko@perimetrix.com>
Date: Tue, 06 Apr 2013 16:02:43 +0300
Subject: план разработки

Во вложении последняя версия плана.
```

Андрей Татаренко

ИО: объект классифицирован, уровень "Разработка/С3"

ИД: Анатолий Бобылев, разрешенный уровень "Разработка/С4"

ВКП: Андрей Татаренко, разрешенный уровень "*/С4"

КП: почтовый ящик @perimetrix.com, разрешенный уровень "*/*"

НЕРАЗРЕШЕННОЕ ДЕЙСТВИЕ С КЛАССИФИЦИРОВАННЫМ ОБЪЕКТОМ

Анатолий Бобылев

```
MAIL FROM:<anatoli.bobylev@perimetrix.com>
RCPT TO: <andrey.tatarenko@gmail.com>
DATA
From: Anatoli Bobylev <anatoli.bobylev@perimetrix.com>
To: Andrey Tatarenko <andrey.tatarenko@gmail.com>
Date: Tue, 06 Apr 2013 16:02:43 +0300
Subject: план разработки

Во вложении последняя версия плана.
```

Андрей Татаренко

ИО: объект классифицирован, уровень "Разработка/С3"

ИД: Анатолий Бобылев, разрешенный уровень "Разработка/С4"

ВКП: Андрей Татаренко, разрешенный уровень "*/С4"

КП: внешний почтовый ящик, разрешенный уровень "-/-"

ОЖИДАНИЯ РУКОВОДСТВА ОТ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

НАДЕЖДЫ:

- ✓ Воспрепятствует краже информации, ее обесцениванию путем разглашения
- ✓ Наведет порядок при работе с ценной информацией
- ✓ Повысит персональную ответственность сотрудников и руководителей за сохранность ценность информации на предприятии
- ✓ Позволит в судебном порядке взыскивать с виновных ущерб от утечки информации

СТРАХИ:

- ☐ ~~Может мешать рабочим процессам, критично сказываться на производительности~~
- ☐ ~~Потребует от сотрудников дополнительных затрат времени на бюрократические процедуры~~
- ☐ ~~Негативно повлияет на атмосферу в коллективе, снизит мотивацию к труду~~
- ☐ ~~Потребует увеличения численности служб безопасности и иных затрат на помещения, оборудование, ПО и др. технические меры~~
- ☐ ~~При неправильной реализации не защитит ценную информацию, затруднит использование «простой» информации~~

ПРИНЦИПИАЛЬНЫЕ ОСОБЕННОСТИ ПОДХОДА PERIMETRIX

- ПРОАКТИВНЫЙ ПОДХОД К БОРЬБЕ С УТЕЧКАМИ
- ЗАЩИТА НЕ МЕНЯЕТ РАЗРЕШЕННЫЕ РАБОЧИЕ ПРОЦЕССЫ
- ЛОГИКА МНОГОМЕРНОЙ КЛАССИФИКАЦИИ ПОНЯТНА ВЛАДЕЛЬЦАМ ДАННЫХ
- МОДЕЛЬ ПРИНЯТИЯ РЕШЕНИЙ УНИВЕРСАЛЬНА И НЕ ЗАВИСИТ ОТ СПЕЦИФИКИ КАНАЛОВ ПЕРЕМЕЩЕНИЯ ИНФОРМАЦИИ
- МЕХАНИЗМ НАСЛЕДОВАНИЯ КАТЕГОРИЙ РЕШАЕТ ЗАДАЧУ КЛАССИФИКАЦИИ ПРОИЗВОДНЫХ ДОКУМЕНТОВ

1 ОРГАНИЗАЦИЯ ПРОЕКТА И СОЗДАНИЕ ТЕСТОВОГО СТЕНДА

- Создание совместной рабочей группы
- Разработка и подписание Меморандума проекта
- Установка системы Perimetrix SafeUse на тестовом стенде
- Обучение специалистов заказчика, включенных в рабочую группу

ИТОГИ ЭТАПА:

- ✓ Определен состав рабочей группы
- ✓ Создан тестовый стенд с системой
- ✓ У заказчика есть **собственные специалисты**, способные транслировать политики безопасности предприятия во внутренние настройки системы

2 ПОСТРОЕНИЕ МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

- Разработка модели угроз утечки классифицированных данных (КД)
- Разработка политик и процедур в части обработки, хранения и передачи КД
- Моделирование новых/скорректированных бизнес-процессов и процедур
- Настройка и симуляция модели защиты информации на тестовом стенде
- Документирование модели защиты информации

ИТОГИ ЭТАПА:

- ✓ Определена и построена **модель защиты**, включающая:
  - ✓ Политики обработки ценных данных
  - ✓ Категории и правила классификации
  - ✓ Полномочия пользователей, приложений
  - ✓ Выполняемые под контролем системы бизнес-процессы и процедуры

3 ОПЫТНАЯ ЭКСПЛУАТАЦИЯ СИСТЕМЫ

- Разработка и утверждение регламента (режима) работы с КД
- Разработка инструкций и обучение пользователей
- Инсталляция и настройка системы на рабочем сервере и станциях пользователей
- Первичная инвентаризация и классификация информационных ресурсов
- Опытная эксплуатация системы

ИТОГИ ЭТАПА:

- ✓ Пользователи предприятия обучены работе в защищенном режиме
- ✓ Система применена в рабочим ресурсам
- ✓ Выявлены замечания и определены корректировки работы системы

4 ВВОД В ПРОМЫШЛЕННУЮ ЭКСПЛУАТАЦИЮ

- Корректировка настроек и процедур по результатам опытной эксплуатации, введение периодических процедур (заданий) в систему
- Разработка и утверждение финальной версии модели защиты информации
- Корректировка и утверждение регламента работы с КД и других документов
- Сдача проекта заказчику

ИТОГИ ЭТАПА:

- ✓ Сотрудники работают с КД в защищенном режиме
- ✓ Разработаны регламенты работы с КТ в ИС и порядок выполнения обслуживающих процедур
- ✓ Специалисты заказчика самостоятельно вносят необходимые изменения в систему защиты

PERIMETRIX®

Российская компания, нацеленная на разработку решений для реализации режима секретности конфиденциальных данных.

КЛИЕНТЫ КОМПАНИИ:

НЕФТЬ И ГАЗ:
ГАЗПРОМ ТРАНСГАЗ ЕКАТЕРИНБУРГ (РОССИЯ)
ГАЗПРОМ НЕФТЬ ШЕЛЬФ (РОССИЯ)
ГАЗПРОМ ДОБЫЧА ШЕЛЬФ (РОССИЯ)
ГАЗПРОМ ИНВЕСТ ЮГ (РОССИЯ)
ГОС. СЕКТОР:
СОВЕТ ФЕДЕРАЦИИ РФ (РОССИЯ)
АДМИНИСТРАЦИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ (РОССИЯ)
УПРАВЛЕНИЕ СЛУЖБЫ СУДЕБНЫХ ПРИСТАВОВ (РОССИЯ)
ARMSCOR (ЮАР)
ФИНАНСЫ:
УКРЭКСИМ БАНК (УКРАИНА)
LIGHTSTONE (ЮАР)
FIC (FINANCIAL INTELLIGENCE CENTER) (ЮАР)
ТЕЛЕКОММУНИКАЦИИ И ТЕХНОЛОГИИ:
МТС (РОССИЯ, БЕЛАРУСЬ)
BLUE LABEL DATA (ЮАР)
ИНТЕГРАЛ (БЕЛАРУСЬ)
МАШИНОСТРОЕНИЕ:
АВТОВАЗ (РОССИЯ)
ЭНЕРГЕТИКА:
РУСГИДРО (РОССИЯ)
ОГК 3 (РОССИЯ)
МЕДИЦИНА:
ПОЛИКЛИНИКА ГАЗПРОМ (РОССИЯ)
ФГУБЗ «ЦЕНТР КРОВИ» ФМБА (РОССИЯ)

НТКС

Партнер компании Perimetrix
в статусе
Channel Partner (Value Added Reseller)
и
System Integrator/Service Partner