«Автоматизация регулярных процессов и рутинных операций управления безопасностью процессов обработки ПДн»

Виды требований в области ПДн

Учет и ведение документации

Обеспечение защиты ресурсов обрабатывающих ПДн

Выполнение требований к процессам обработки ПДн

Контроль соответствия форм и процессов обработки ПДн требованиям

Прием и обработка запросов субъектов ПДн и регулирующих органов

Документы

- Модель угроз и модель нарушителя
- Описание системы защиты
- Уведомление об обработке ПДн
- Акт классификации ИСПДн
- Перечень ПДн
- . . .

Актуальны?

Журналы, приказы…

Учет машинных носителей ПДн

Учет эксплуатационной документации

Учет средств защиты

Учет ключевых носителей

Приказы на допуск к ПДн, СКЗИ

. . .

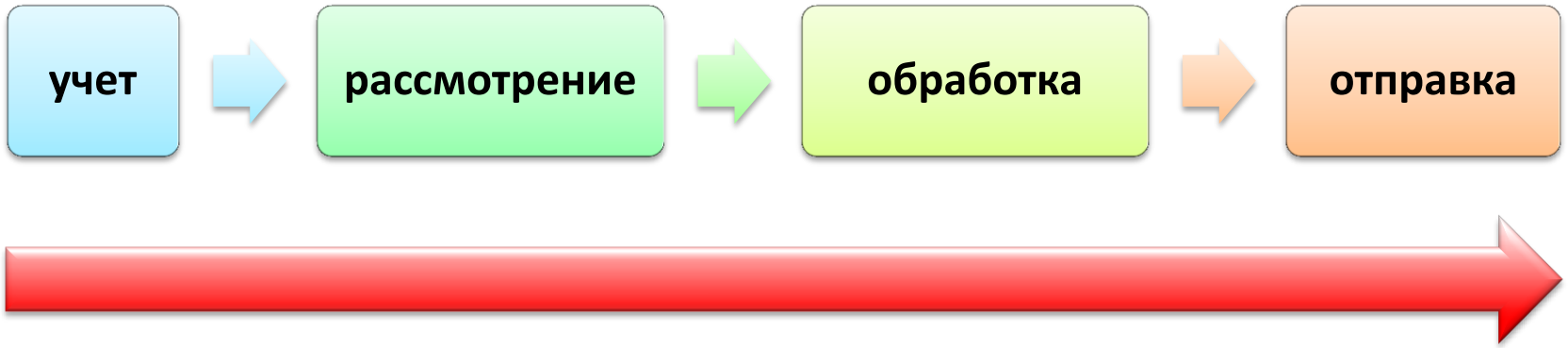
Работа с субъектами ПДн

Учет обращений граждан с жалобами, запросами, претензиями…

Рассмотрение обращений, принятие по ним решений

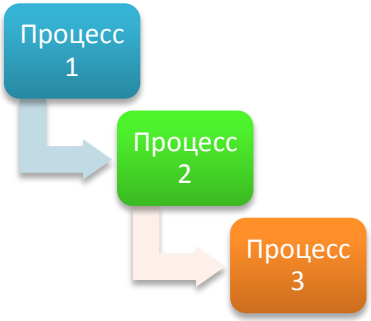
Выполнение решений

Отправка уведомлений, разъяснений по результатам рассмотрения обращений



Система сбора информации

Система анализа информации



Документация

- Модель угроз
- Описание системы защиты
- Уведомление об обработке ПДн…

Состав, конфигурация средств защиты ПДн

Мероприятия по защите ПДн

- Обучение
- Проверка лояльности
- Допуск к обработке ПДн…

Формы для субъектов ПДн

- Формы согласий на обработку ПДн
- Формы разъяснений
- Формы уведомлений…

Содержание договоров с третьими лицами

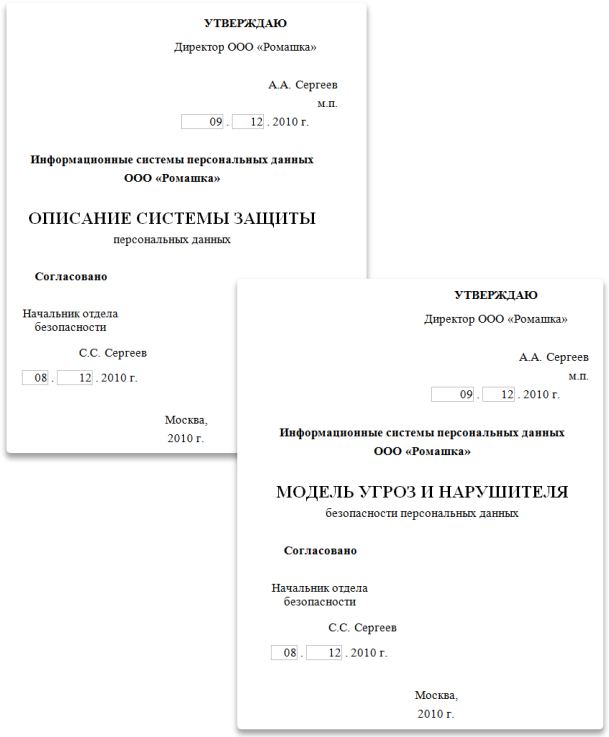
Система актуализации и подготовки документов

Подготовка (адаптация) документа

Согласование документа

Печать документа

Утверждение документа



УТВЕРЖДАЮ
Директор ООО «Ромашка»
А.А. Сергеев
м.п.
09 . 12 . 2010 г.

Информационные системы персональных данных ООО «Ромашка»

ОПИСАНИЕ СИСТЕМЫ ЗАЩИТЫ
персональных данных

Согласовано
Начальник отдела безопасности
С.С. Сергеев
08 . 12 . 2010 г.

Москва, 2010 г.

УТВЕРЖДАЮ
Директор ООО «Ромашка»
А.А. Сергеев
м.п.
09 . 12 . 2010 г.

Информационные системы персональных данных ООО «Ромашка»

МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ
безопасности персональных данных

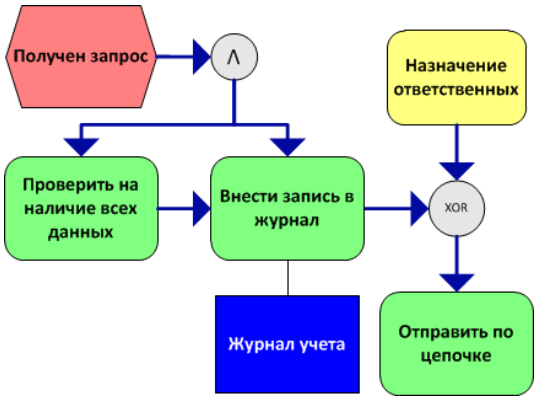
Согласовано
Начальник отдела безопасности
С.С. Сергеев
08 . 12 . 2010 г.

Москва, 2010 г.

Система работы с субъектами ПДн

Процедура учета запросов

- Форма журнала
- Порядок заполнения
- Ответственные



Процедура рассылки

- Анализ содержания запросов
- Адресаты
- Содержание рассылки

Процедура принятия решений

- Анализ содержания запроса
- Необходимые проверки
- Действия по результатами проверки
- Содержание ответа

Процедура подготовки ответа

- Адресаты (субъект, РКН)
- Формы ответа
- Содержание форм
- Сроки отправки

Система внесения изменений в конфигурацию системы защиты

ИСПДн 1

- требование 1
- требование 2

ИСПДн 2

- требование 3
- требование 4

Характер процессов обработки ПДн

- МПО, ОПО
- с РПД или без
- …

Средства защиты ПДн:

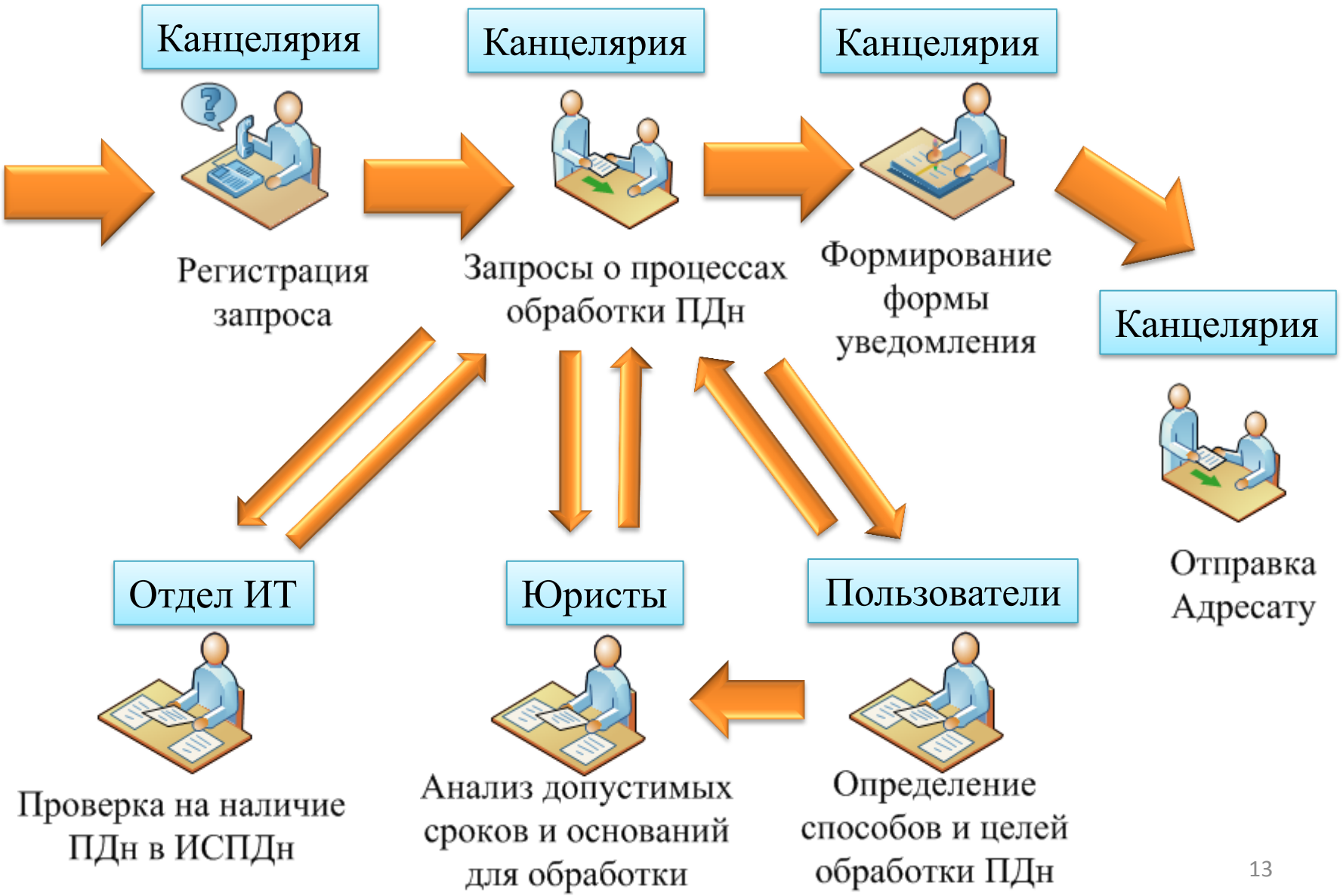
- СЗИ от НСД
- МЭ
- …

Система контроля сроков

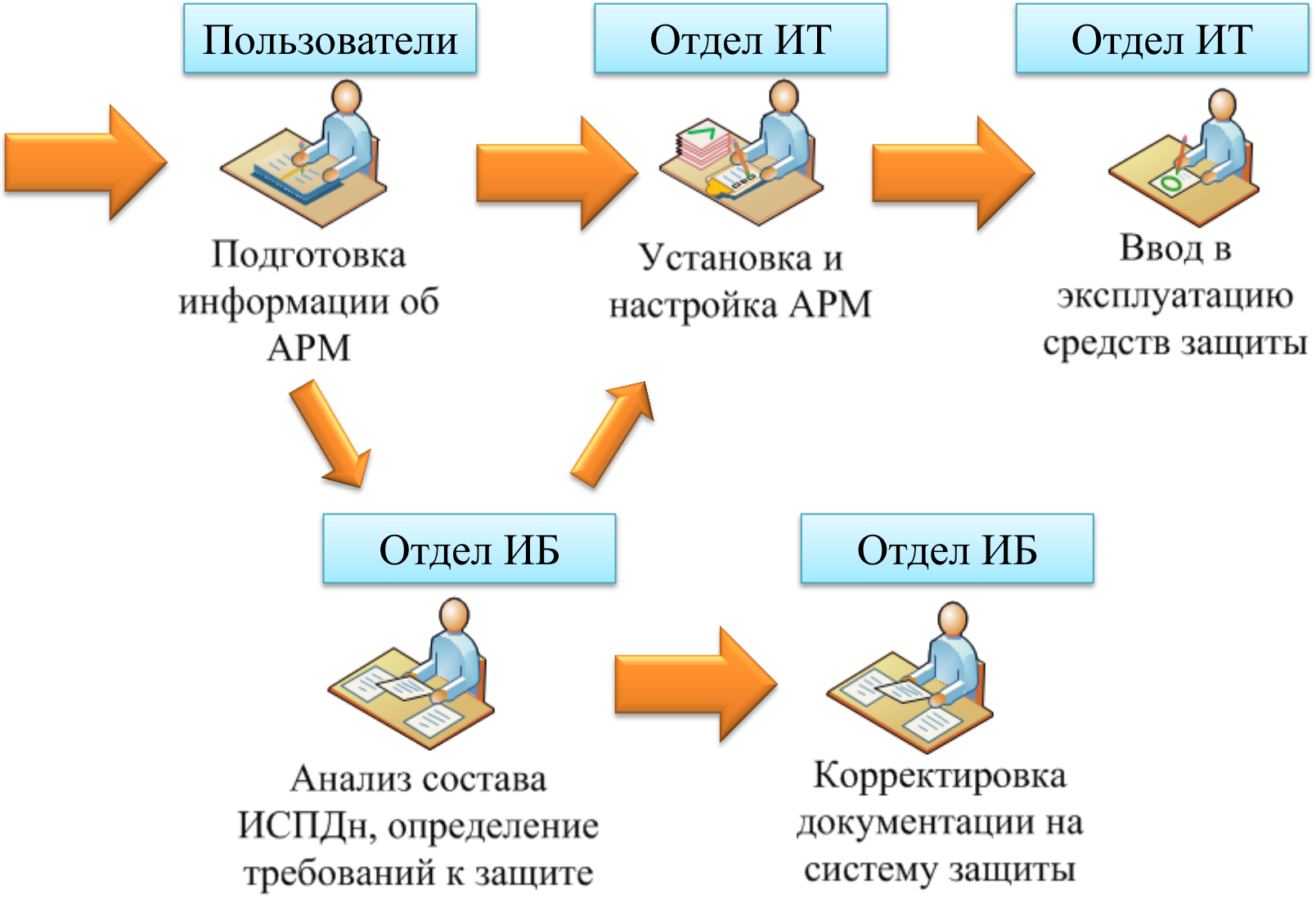
Состав необходимой информации

Сведения о составе и структуре ИС	• Состав АРМ и серверов, их расположение • Состав сетевого и телекоммуникационного оборудования • Используемые носители информации • Состав и характер связей между сетевыми элементами…
Сведения о ПДн	• Состав баз данных, каталогов, бумажных форм содержащих ПДн и их расположение • Состав и объем обрабатываемых ПДн • Состав и направление потоков ПДн • Носитель ПДн: электронный, акустический сигнал, бумажный и т.п. …
Сведения о процессах обработки ПДн	• Способы и цели обработки ПДн, источники получения ПДн • Состав ПДн участвующий в тех или иных процессах • Нормативные основания обработки ПДн • Третьи стороны участвующие в процессах обработки, характер участия • Операции выполняемые с ПДн …
Сведения о лицах	• Состав пользователей ИСПДн • Объем прав доступа имеющийся у пользователей • Состав администраторов ИСПДн, функции и роли администраторов • Состав ответственных за обеспечение безопасности ПДн • Конкретный состав субъектов ПДн в каждой ИСПДн …

Пример запроса по ПДн



Пример запроса на установку



Выводы

Значительные трудозатраты:

- **трудозатраты службы ИТ**
- **трудозатраты службы ИБ**
- **трудозатраты пользовательских подразделений**

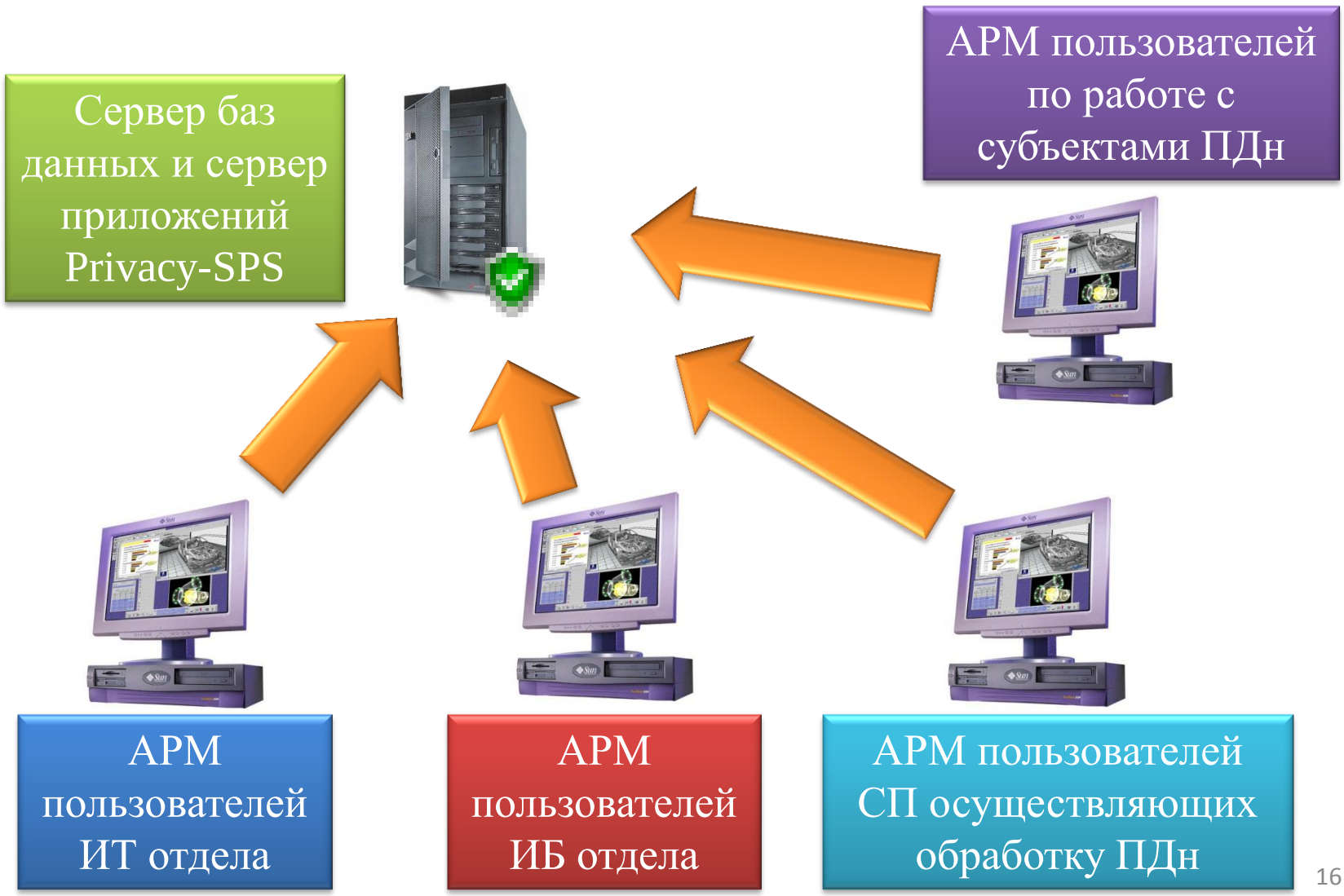
Высокая вероятность:

- **потери нужной информации**
- **некорректного анализа**
- **ошибок при обработке информации**

Претензии регуляторов

Иски субъектов ПДн

Privacy-SPS
Состав и структура комплекса



Privacy-SPS
Ввод данных

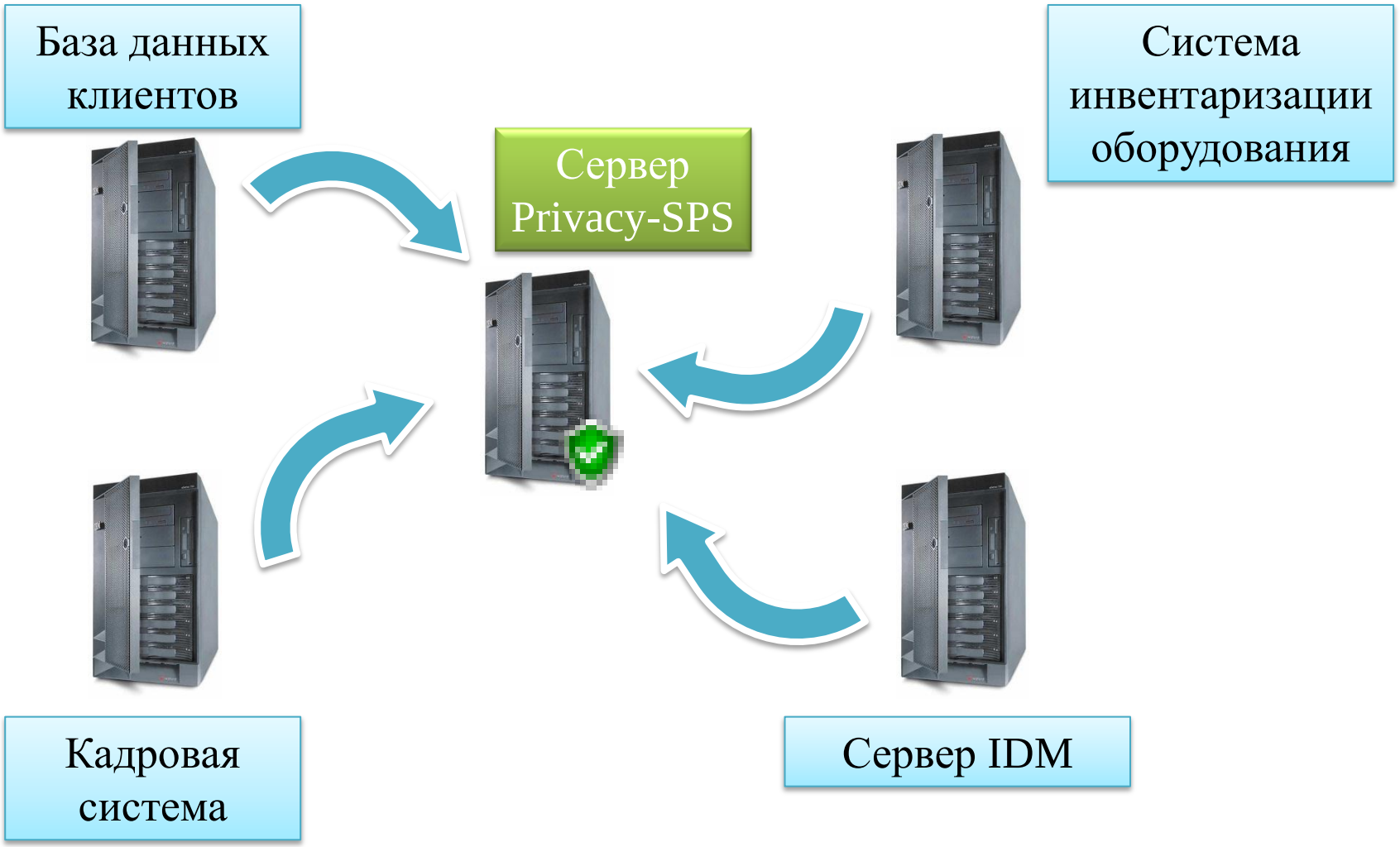
Формализованные формы ввода

Контроль введенных данных

Возможность использования ранее введенной информации

Отсутствие дублирования информации

Privacy-SPS
Интерфейсы к внешним системам

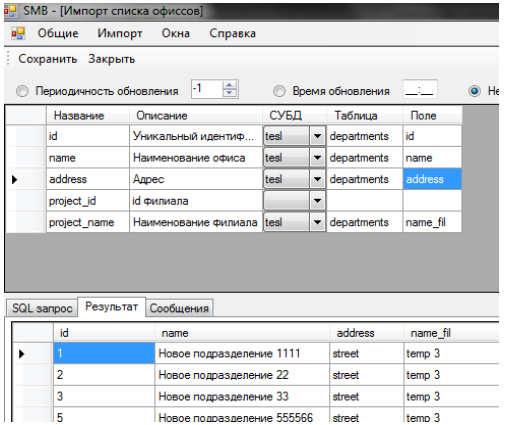


Privacy-SPS
Работа интерфейса

IRADD

Обновление данных в системе

Доступ к внешней базе данных



Загрузка данных в промежуточное хранилище

Обработка данных

Privacy-SPS
Анализ и контроль данных

IRADD

Необходимость корректировки документов

Контроль сроков выполнения мероприятий

Анализ данных по результатам ввода

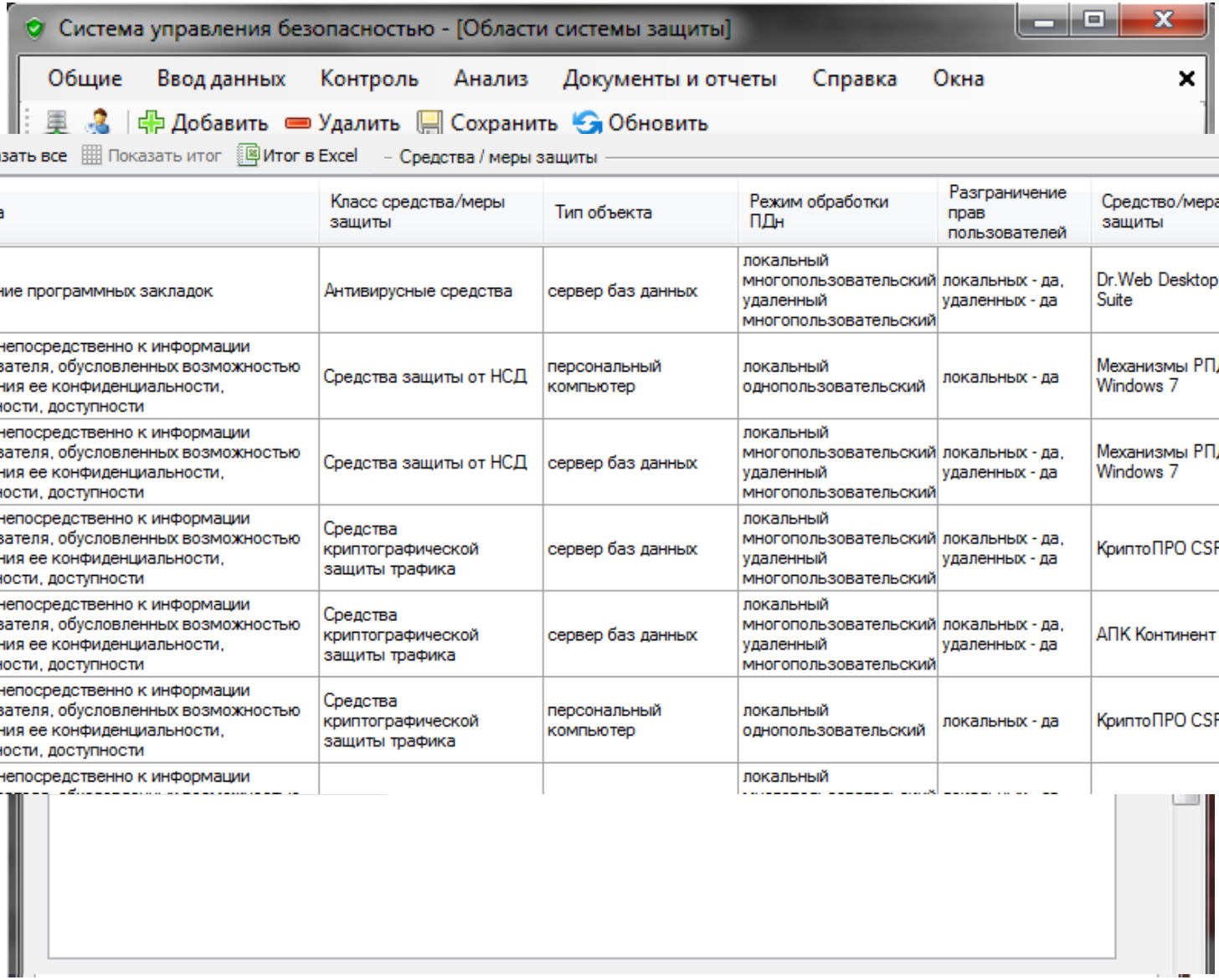
Необходимость отправки ответов на запросы

Необходимость ввода дополнительных данных

Необходимость выполнения мероприятий по защите, обработке ПДн

Более 30 контролей

Privacy-SPS
Выбор варианта защиты ПДн



Угроза	Класс средства/меры защиты	Тип объекта	Режим обработки ПДн	Разграничение прав пользователей	Средство/мера защиты	V
внедрение программных закладок	Антивирусные средства	сервер баз данных	локальный многопользовательский удаленный многопользовательский	локальных - да, удаленных - да	Dr.Web Desktop Security Suite	☑
доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности	Средства защиты от НСД	персональный компьютер	локальный однопользовательский	локальных - да	Механизмы РПД ОС Windows 7	☑
доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности	Средства защиты от НСД	сервер баз данных	локальный многопользовательский удаленный многопользовательский	локальных - да, удаленных - да	Механизмы РПД ОС Windows 7	☑
доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности	Средства криптографической защиты трафика	сервер баз данных	локальный многопользовательский удаленный многопользовательский	локальных - да, удаленных - да	КриптоПРО CSP	☑
доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности	Средства криптографической защиты трафика	сервер баз данных	локальный многопользовательский удаленный многопользовательский	локальных - да, удаленных - да	АПК Континент	☑
доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности	Средства криптографической защиты трафика	персональный компьютер	локальный однопользовательский	локальных - да	КриптоПРО CSP	☑
доступ непосредственно к информации			локальный			

Privacy-SPS
Генерация документов

- Модель угроз и нарушителя по требованиям ФСТЭК России
- Акт классификации
- Приказы на допуск к ПДн и СКЗИ
- Описание системы защиты
- Журнал учета средств защиты, журнал учета носителей ПДн
- Уведомление об обработке ПДн Роскомнадзора
- Приказ на проведение контроля защищенности, акт о результатах
- Заключения о готовности средств защиты к эксплуатации, приказы на ввод в эксплуатацию
- формы Уведомлений, согласий и т.п. …

Порядка 30 видов документов

Privacy-SPS
Работа с субъектами ПДн

IRADD

База данных клиентов

Сведения о наличии ПДн субъекта

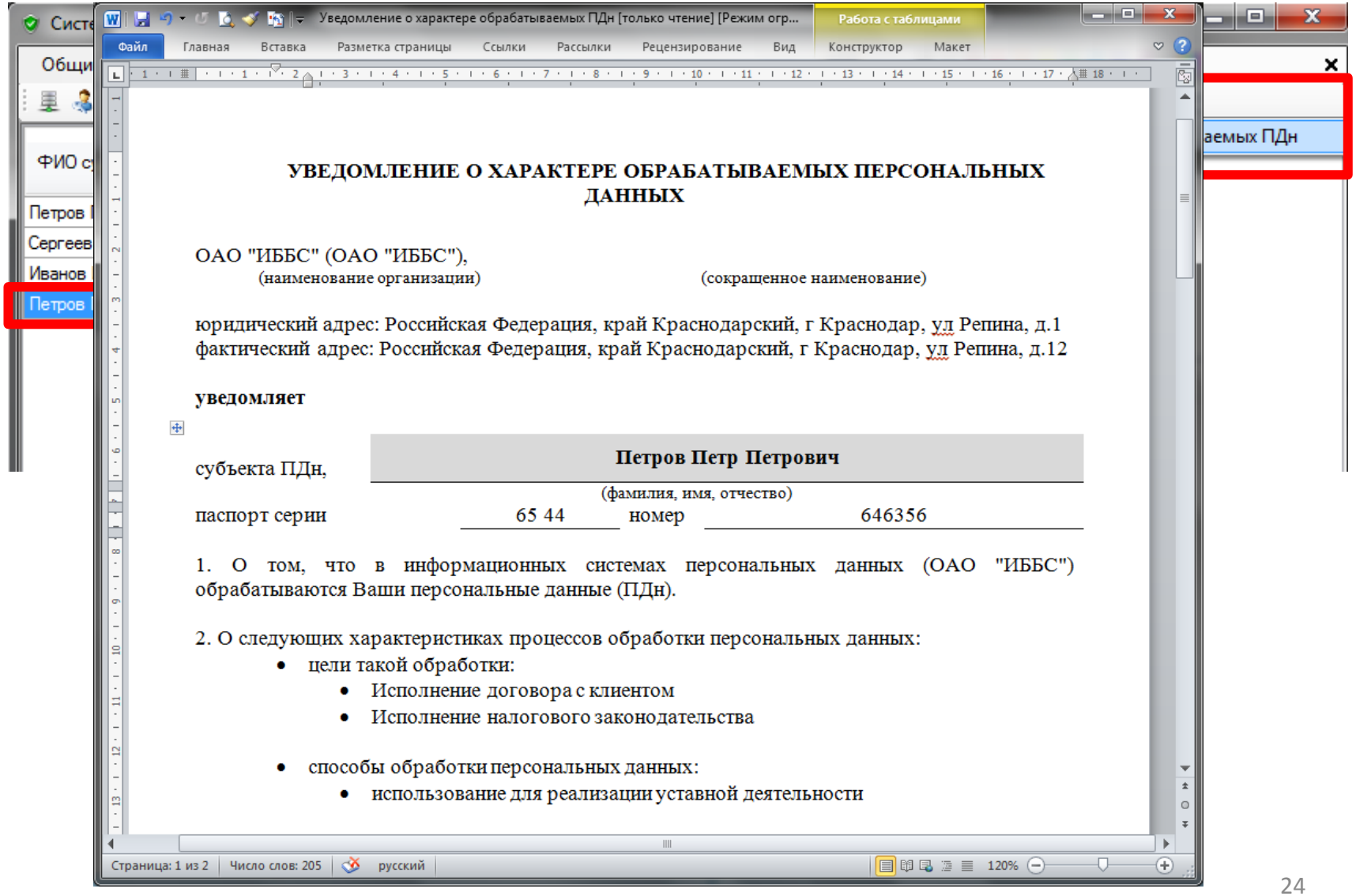
Анализ состава запроса, определение необходимой формы ответа

Автоматическая выдача формы документа

База данных сотрудников

База данных поставщиков

Privacy-SPS
Пример обработки запроса



Privacy-SPS
Координация действий

IRADD

Ввод данных подразделением 1

Автоматическое определение проблем на данном уровне

Решение проблем подразделением 2

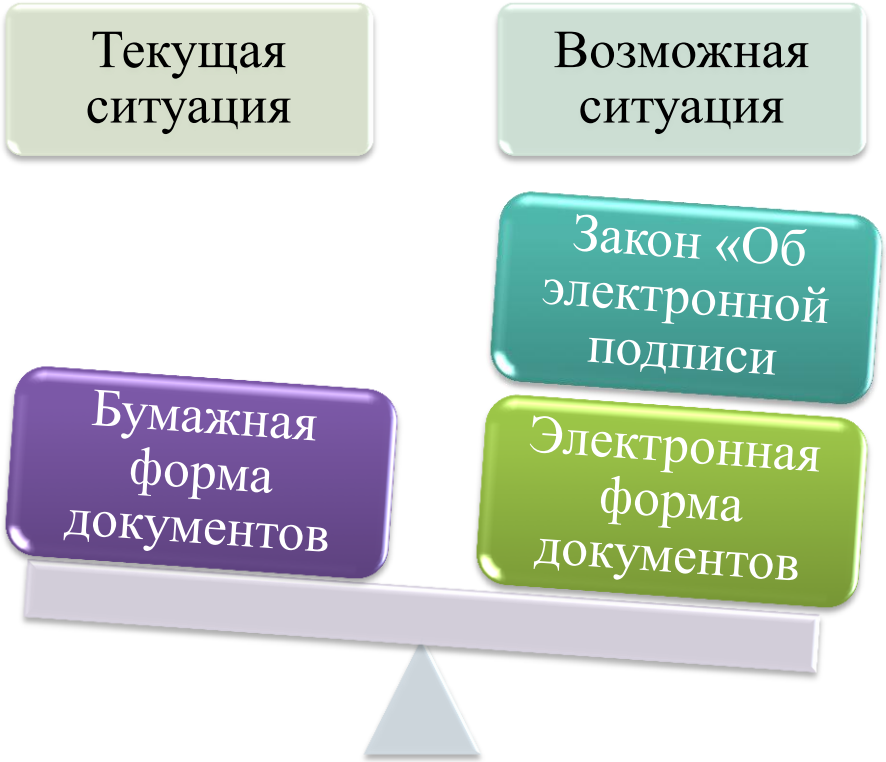
Автоматическое определение проблем на новом уровне

Решение проблем подразделением 3

Инструкция

Функция	Ответственный
Ввод данных по запросам субъектов ПДн	Канцелярия
Ввод данных по способам обработки ПДн	Подразделения участвующие в обработке ПДн
Ввод данных по составу серверов	Отдел ИТ
…	…

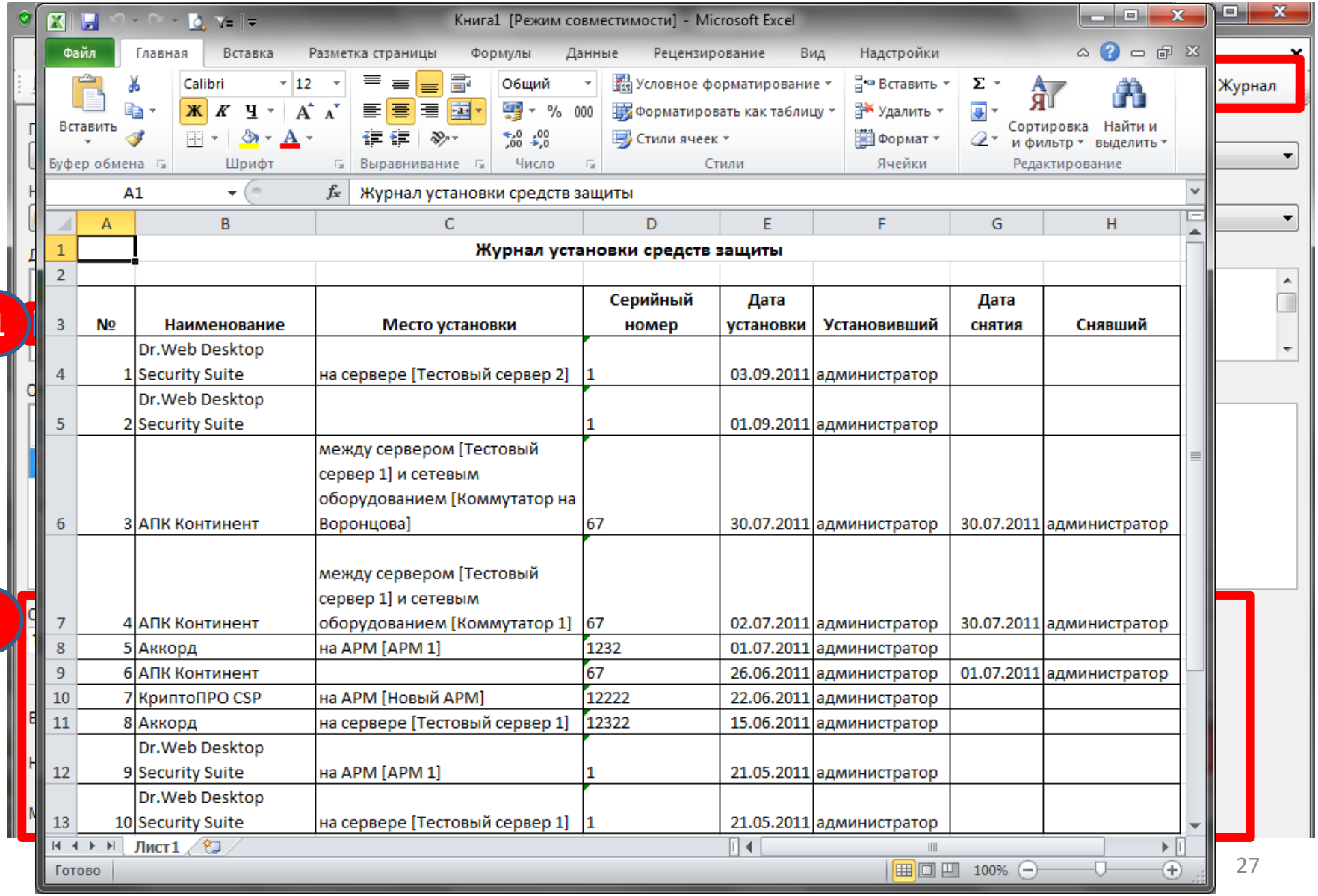
Privacy-SPS
Ведение журналов, документов



Журналы учета (носителей, запросов субъектов ПДн, средств защиты и т.п.)

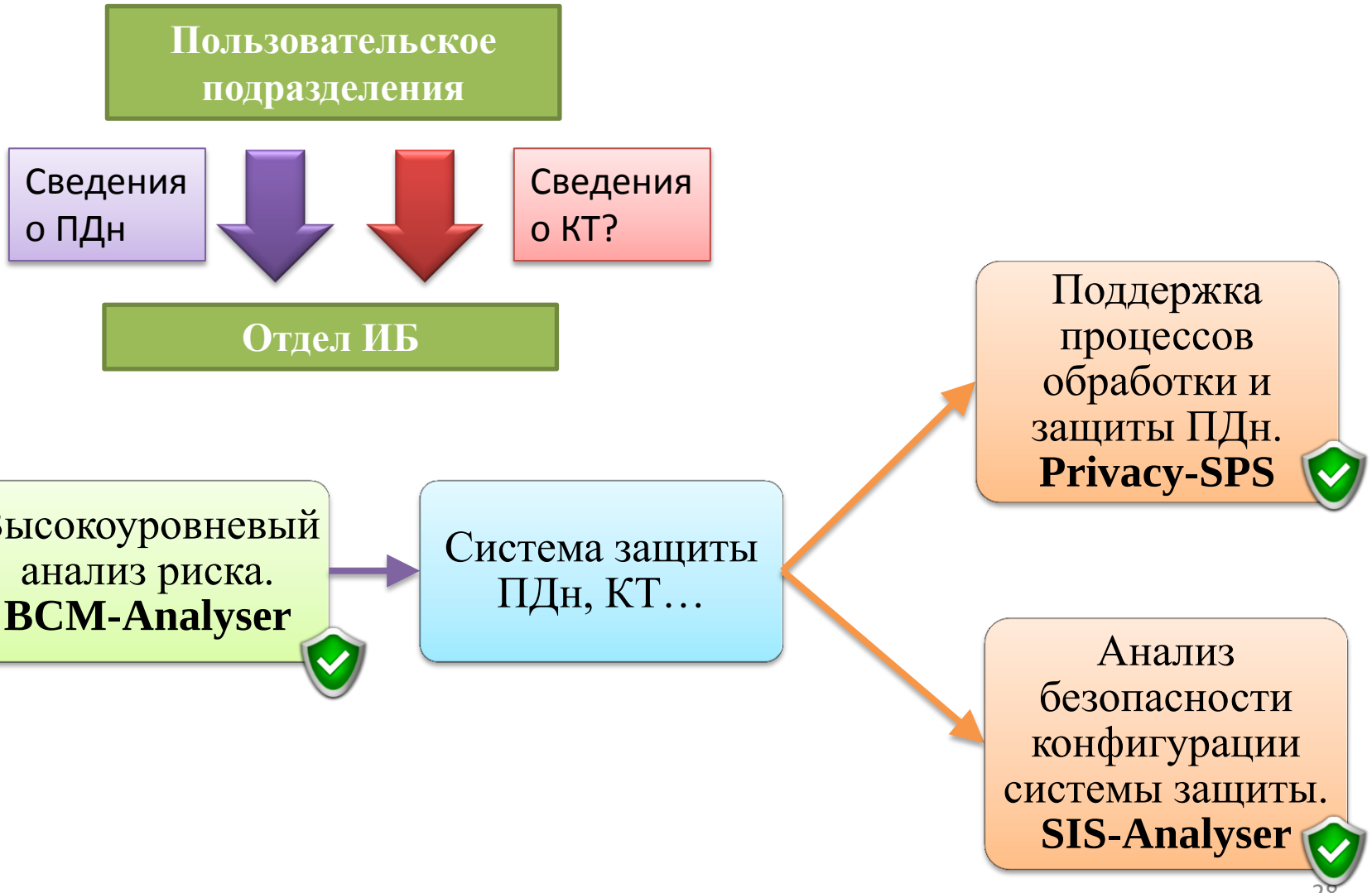
Документы (модель угроз, акт классификации, описание системы защиты)

Privacy-SPS
Пример ведения журнала



№	Наименование	Место установки	Серийный номер	Дата установки	Установивший	Дата снятия	Снявший
1	Dr.Web Desktop Security Suite	на сервере [Тестовый сервер 2]	1	03.09.2011	администратор		
2	Dr.Web Desktop Security Suite		1	01.09.2011	администратор		
3	АПК Континент	между сервером [Тестовый сервер 1] и сетевым оборудованием [Коммутатор на Воронцова]	67	30.07.2011	администратор	30.07.2011	администратор
4	АПК Континент	между сервером [Тестовый сервер 1] и сетевым оборудованием [Коммутатор 1]	67	02.07.2011	администратор	30.07.2011	администратор
5	Аккорд	на АРМ [АРМ 1]	1232	01.07.2011	администратор		
6	АПК Континент		67	26.06.2011	администратор	01.07.2011	администратор
7	КриптоПРО CSP	на АРМ [Новый АРМ]	12222	22.06.2011	администратор		
8	Аккорд	на сервере [Тестовый сервер 1]	12322	15.06.2011	администратор		
9	Dr.Web Desktop Security Suite	на АРМ [АРМ 1]	1	21.05.2011	администратор		
10	Dr.Web Desktop Security Suite	на сервере [Тестовый сервер 1]	1	21.05.2011	администратор		

Privacy-SPS
BCM-Analyser, SIS-Analyser



Вопросы

ООО «АйРЭД»
тел./факс: (861) 274-69-84
e-mail: mail@iradd.ru
www.iradd.ru