ОТ DLP К IRM ПРАКТИКЕ

(СЛУЖБА УПРАВЛЕНИЯ ПРАВАМИ)

softline® 20+ Years in IT

8 (800) 100-00-23 www.softlinegroup.com

info@softline.ru | info@softlinegroup.com

АЛЕКСЕЙ ТИТКОВ

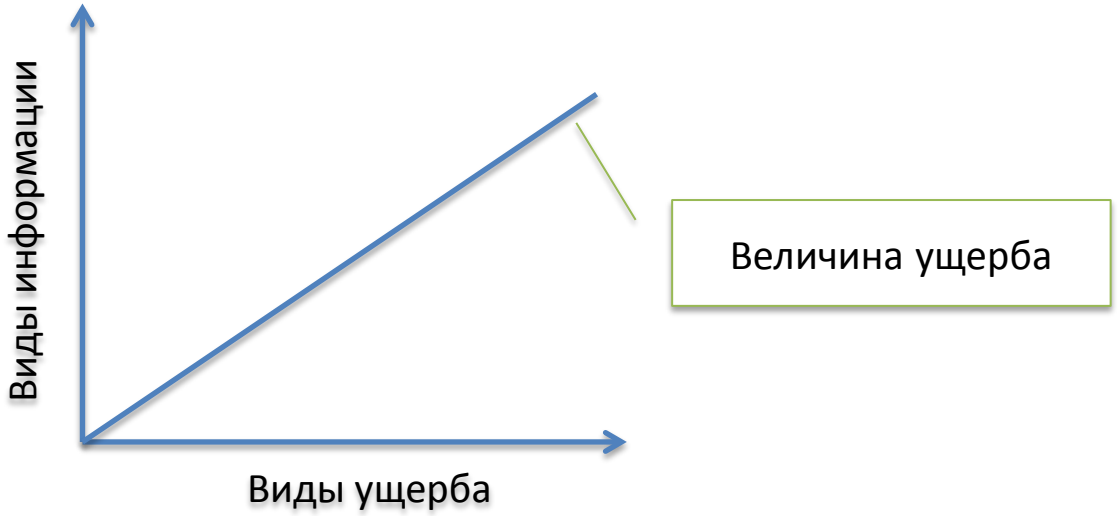
SSM SOFTLINE

Вопросы

- Как обезопасить и контролировать копии?
- Как предотвратить неправомочную пересылку и редактирование копий?
- Как защитить конфиденциальную информацию, передаваемую партнёрам, поставщикам и клиентам?
- Как отменить доступ, когда проект завершён или сотрудник уволен?
- Как контролировать версии используемых документов?

Виды ущерба от потери информации

- Прямое списание стоимости активов
- Компенсационные платежи контрагентам
- Расходы, связанные с судебными разбирательствами и иные юридические платежи
- Штрафы и иные обязательные платежи
- Упущенная прибыль
- Нарушение внутренних процессов
- Потеря репутации или других параметров, приводящих в дальнейшем к потере клиентской базы
- Приостановка деятельности



Решение класса IRM

Кто из сотрудников может использовать информацию?

- Доступ есть
- Достуа нет

Что может делать с информацией каждый сотрудник?

- В локальном ДА
- За периметром НЕТ

Что может делать с информацией каждый сотрудник?

- Смотреть ДА
- Копировать НЕТ
- Печать НЕТ

Когда сотрудник имеет доступ к информации?

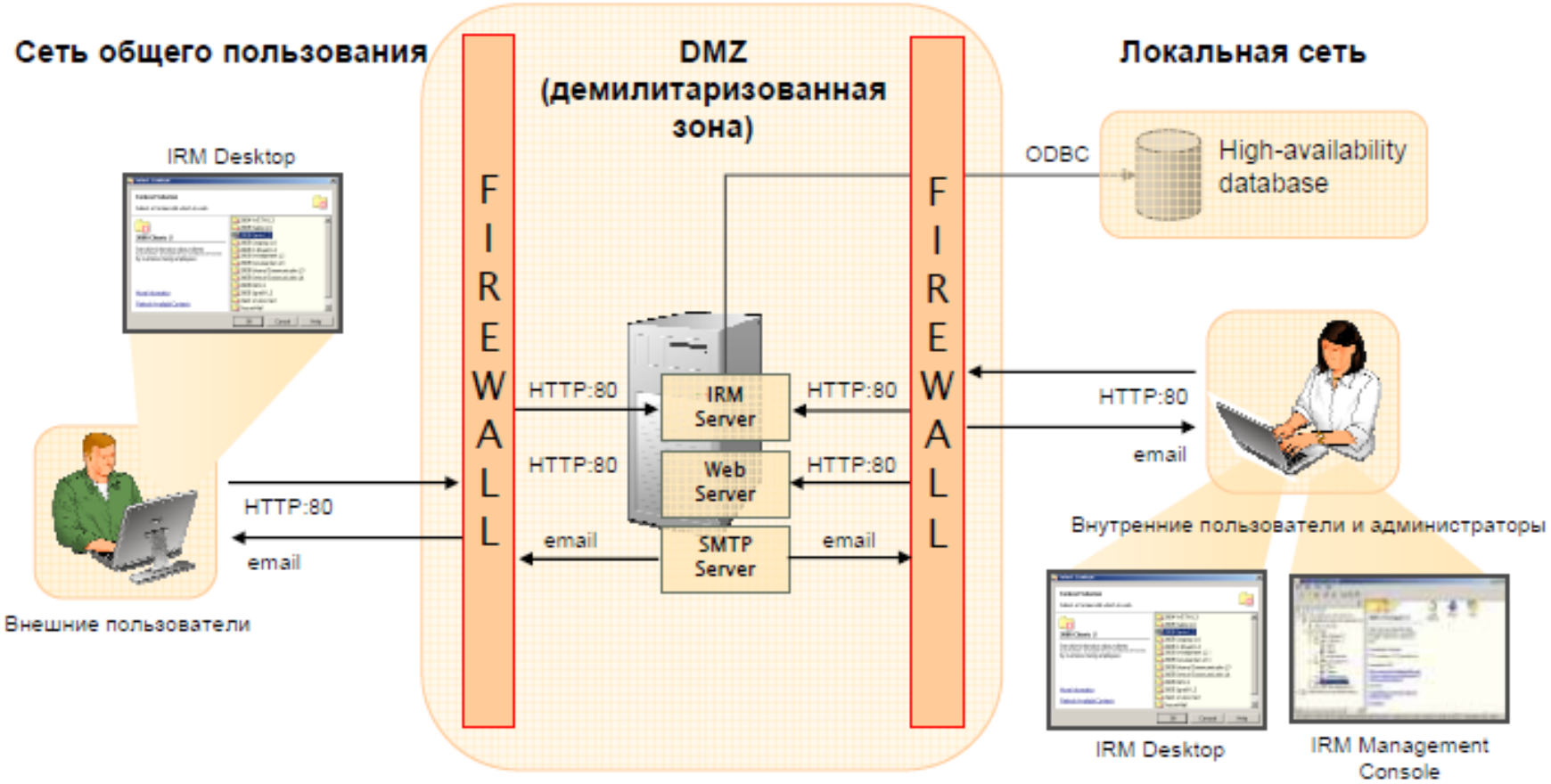
- В это время ДА
- В это время НЕТ

Типовая архитектура

- Все сотрудники могут немедленно получить права/роли
- Внешние пользователи могут получать роли на основе web-доступа
- Наиболее критичная информация может быть опечатана
- Требуется лишь нажать ещё одну кнопку «ОК» для создателей информации (теперь всё контролируется и права можно изъять)
- Создатель бизнес-процесса связывает роли пользователей и группы пользователей
- Нет необходимости привлекать IT-специалистов
- Часто контроль ведётся секретарями

Эффективная безопасность требует ПРОСТОТЫ

Функциональность: схема работы



Плюсы

- обеспечение защиты выбранных документов
- только обладая соответствующими правами возможно открыть/редактировать документ
- документ можно изъять из обращения
- доступ и регистрация документов в системе централизована

Минусы

- риск потери доступа ко всем защищаемым документам
- необходимость снятие защиты для обмена данными с внешними контрагентами
- отсутствие классификации, распознавания дублей
- отсутствие сертифицированной в РФ криптографии

Модель угроз – на уровне АРМ

Действие	Вероятность реализации	Вероятность реализации
Передача через мессенджеры	Инцидент	Высокая
Передача через Браузер	Инцидент	Высокая
Передача через FTP-клиент	Инцидент	Средняя
Передача по e-mail	Инцидент	Высокая
Вынос оборудования или СН	Инцидент	Высокая
Копирование на удаленную РС	Инцидент	Высокая
Печать	Инцидент	Высокая

Интеграция с DLP

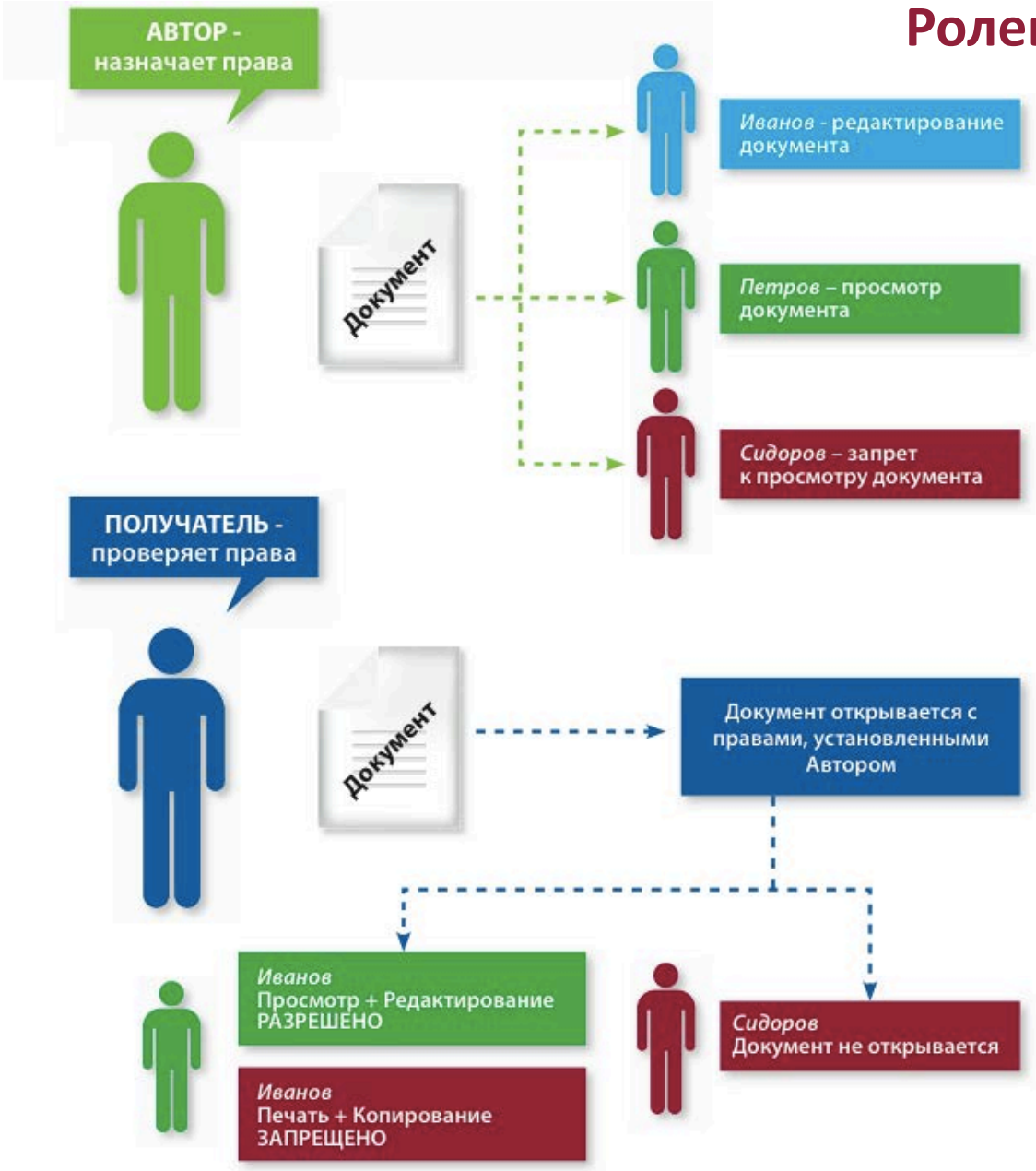
Пользователю назначают права на доступ к конфиденциальному документу, после чего документ контролируется IRM системой

В случае не назначения пользователем прав на доступ к документу, осуществляется попытка отправки документа с ПК по каналам связи (почта, интернет, съемные носители и т.д.)

DLP система **заблокирует** отправку документа или перенаправит его на шлюз шифрования IRM системы после чего документ уйдет **защищенным**.

Открытие такого защищенного документа на неавторизованных рабочих местах за пределами организации будет **невозможна**.

Ролевая модель



Производители

SECLORE

Microsoft

Adobe

ORACLE