softline®
Мы всё сможем
30 лет в ИТ

Трансформация.
Успешная. Цифровая. Защищенная.

Технологический час с экспертом
Защита КИИ сегодня.

Захар Пожидаев
Менеджер по продажам решений
Департамент информационной безопасности
M +7 919 772-28-78 | Zakhar.Pozhidaev@softline.com

Спикеры

Руководитель направления безопасности объектов критической информационной инфраструктуры.

Руководитель направления безопасности промышленных предприятий.

Ведущий эксперт блока безопасности промышленных предприятий.

Субъекты и объекты КИИ

Трансформация.
Успешная. Цифровая. Защищенная.

здравоохранение

наука

транспорт

связь

финансы и банки

атомная и топливная энергетика

промышленность (горнодобывающая, оборонная, химическая, металлургическая, ракетно-космическая)

гос. регистрация прав на недвижимое имущество и сделок с ним

Субъекты

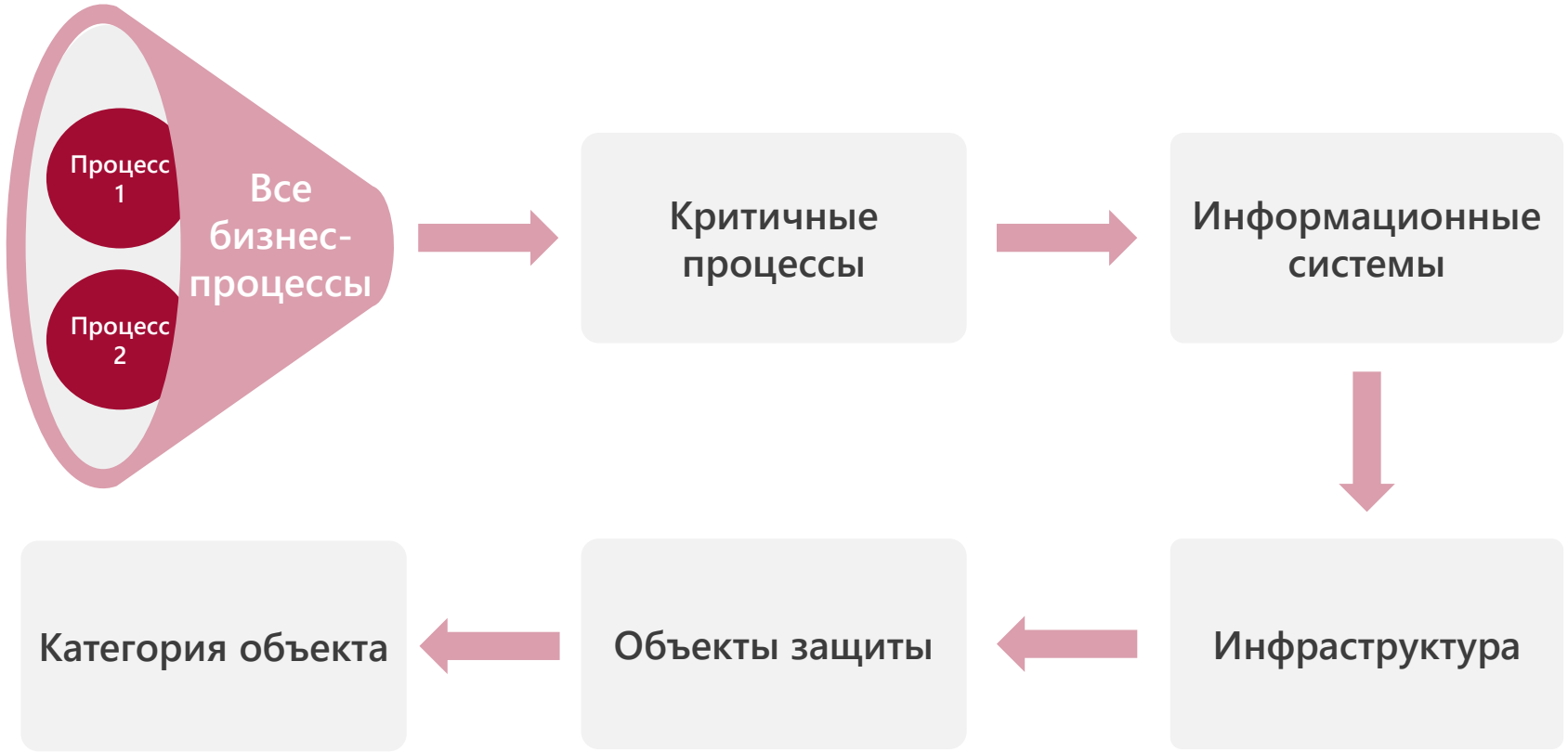
- Гос. Учреждения
- Гос. Органы
- Российские ЮЛ и ИП

Объекты

- информационные системы
- информационно-телекоммуникационные сети
- автоматизированные системы управления

Утвердить до 1 сентября 2019 г. перечень объектов КИИ, подлежащих категорированию + 1 год на работы по Категорированию

Классический пример категорирования

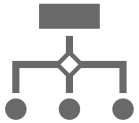


Сопутствующие вопросы:

1. Все ли критичные процессы получилось выявить?
2. Учтены ли все связи объектов?
3. Правильно ли определена категория объектов?
4. Возможно ли понизить категорию? Как обосновать?
5. Достаточно ли для безопасности бизнеса принятых мер ИБ

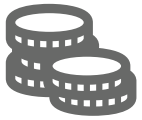
Кому поможет?

Малый и средний бизнес с простой архитектурой



Небольшое количество бизнес-процессов (<5)

Риски ИБ понятны «на глаз» и идентифицированы



Финансовый ущерб не значителен

Выполнение требований Регулятора «для галочки»

Категорирование сложной инфраструктуры.

Часть 1. Обследование

Категорирование сложной инфраструктуры.

Часть 2. Анализ собранной информации

Категорирование сложной инфраструктуры.

Трансформация.
Успешная. Цифровая. Защищенная.

Часть 3. Имитационное моделирование и анализ угроз

Категорирование сложной инфраструктуры.

Трансформация.
Успешная. Цифровая. Защищенная.

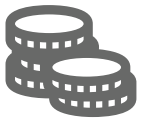
Часть 4. Определение Категории значимости ОКИИ

Кому это нужно

Крупный и средний бизнес со сложной архитектурой

Много бизнес-процессов (>15)

Риски ИБ не идентифицированы совсем, или работа проведена «на глаз»



Нет понимания о реальном финансовом ущербе в случае реализации рисков ИБ

Кейс: Компания А. Проблематика. Задачи

Портрет

1. Крупный объект промышленности
2. Часть объекта на этапе строительства. Поэтапная сдача объектов строительства
3. Сложная распределенная архитектура (порядка 150 ИС и АСУ ТП)
4. Собственники систем – разные юридические лица
5. Отсутствие единой точки входа
6. Проектная и рабочая документация в стадии разработки
7. Замечания от Регулятора по предыдущему категорированию
8. Порядка 500 отраслевых требований и требований законодательства к ИБ

Исходные данные

1. Компания самостоятельно проводила категорирование в 2020 году. Часть ОКИИ имела 1 категорию значимости.
2. В 2022 году от отраслевого регулятора поступили запрос о предоставлении актуальной информации о действующих ОКИИ

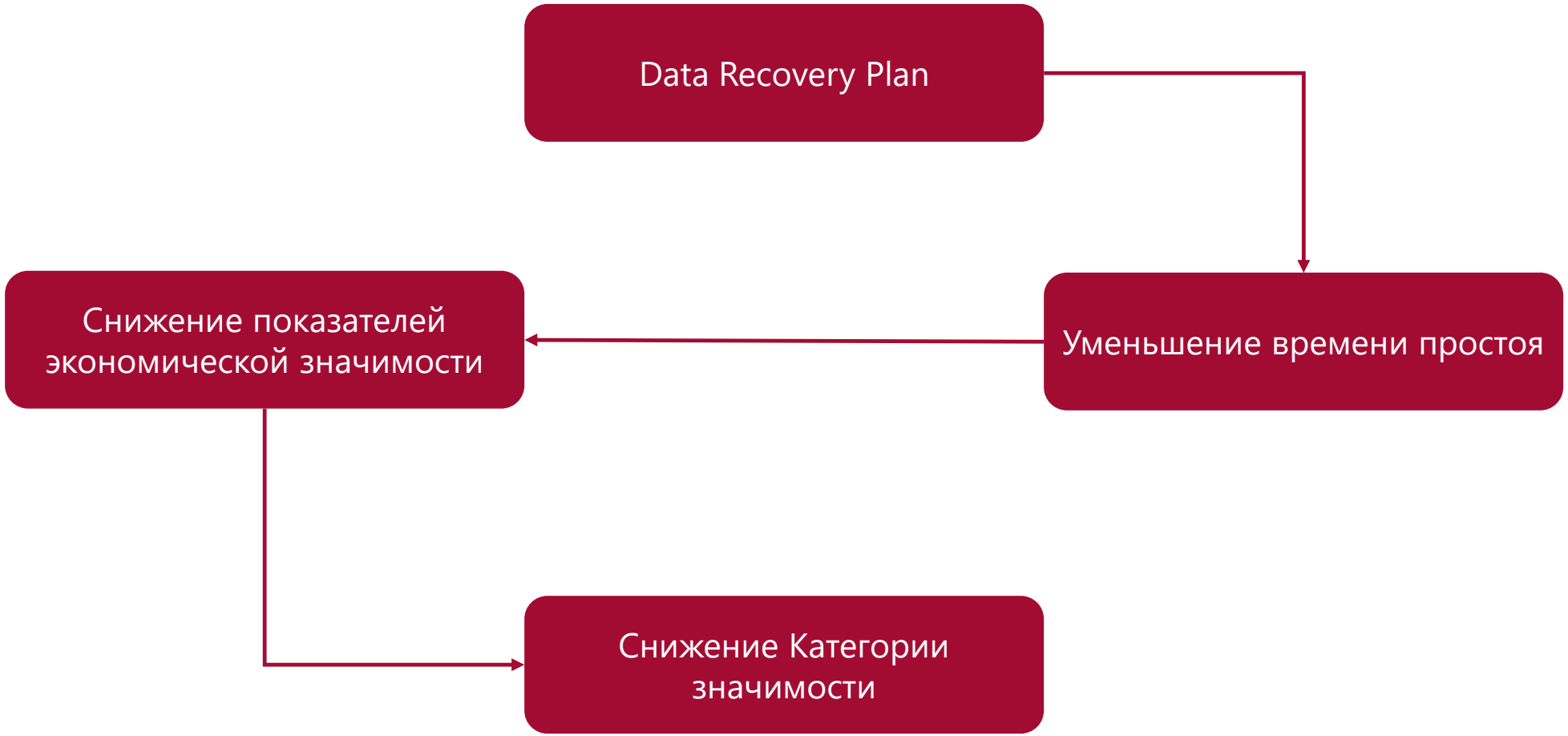
Задача

1. Пересмотреть категории ОКИИ
2. Категорировать новые ОКИИ
3. Обновить модель угроз
4. Спроектировать систему защиты с использованием отечественных СЗИ
5. Предоставить обновленную информацию во ФСТЭК России

Решение. Часть 1.

Решение. Часть 2.

Как DRP связан с категорией ОКИИ



Ключевые артефакты при построении DRP

Recovery Time Objective (RTO) – Целевое время восстановления

Recovery Point Objective (RPO) – Целевая точка восстановления

DRP на практике

Пример

- ✓ Согласованность параметров = нет конфликтов внутри
- ✓ Всегда сможем подтвердить бюджет

ИС	Пара-метр	Интервьюируемые лица	Влияние	1 час	2 часа	4 часа	8 часов	10 часов	12 часов	24 часа	2 дн.	3 дн.	4 дн.	5 дн.	1 нед.	2 нед.	3 нед.	месяц	Минимальный RTO/RPO по каждой анкете
Oracle	RTO	1. …	Финансовый ущерб																10 часов
			Доступность																
			Управляемость																
			Репутация																
		2. …	Управляемость																2 часа
			Репутация																
		3. …	Финансовый ущерб																4 дня
	RPO	1. …	Финансовый ущерб																10 часов
			Доступность																
			Управляемость																
			Репутация																
		2. …	Финансовый ущерб																Не применимо
			Доступность																
			Управляемость																
			Репутация																

Решение. Часть 2.

Кейс: Компания А. Результат

1. Во время обследования были выявлены дополнительные ОКИИ
2. Переработана модель угроз безопасности
3. Пересмотрена категория всех ОКИИ.
4. Часть ОКИИ 1 категории значимости мотивированно были отнесены к 3 категории за счет «Заключения о негативных последствиях» и «Плана аварийного восстановления»
5. Разработан концепт системы защиты с использованием отечественных СЗИ с рекомендациями по его реализации

Трансформация.

Успешная. Цифровая. Защищенная.

www.softline.ru

Мы всё сможем

softline® 30 лет в ИТ

softline®

Мы всё сможем

30 лет в ИТ

Трансформация.

Успешная. Цифровая. Защищенная.

Захар Пожидаев
Менеджер по продажам решений
Департамент информационной безопасности
M +7 919 772-28-78 | Zakhar.Pozhidaev@softline.com