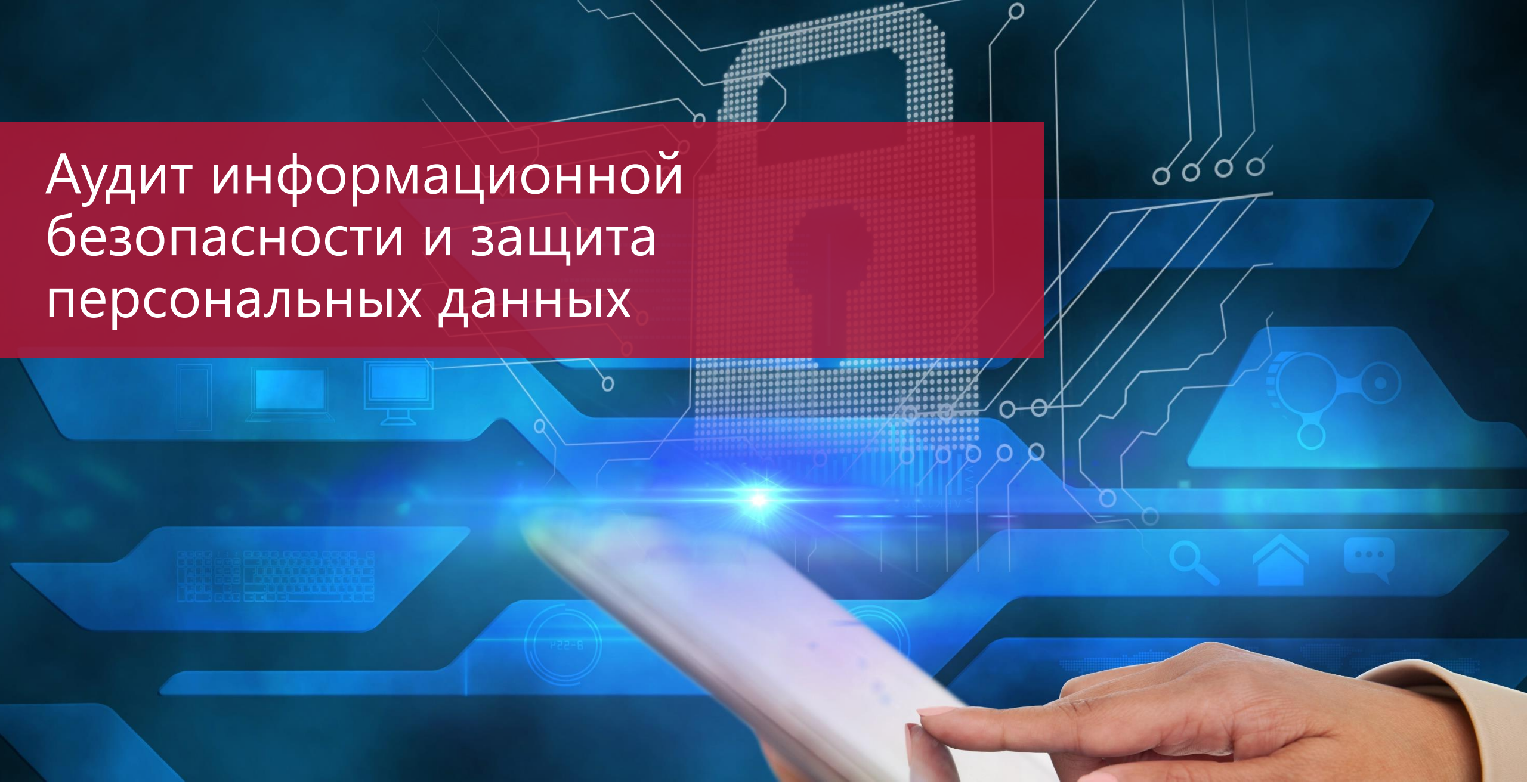
Аудит информационной безопасности и защита персональных данных



Регуляторы в области защиты ПДн

система органов, осуществляющих надзор за соблюдением Конституции и всех законов

уполномоченный орган по защите прав субъектов персональных данных

федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации

федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности

Новые штрафы в КоАП ст.13.11 (с 01.07.2017)

		МИНИМУМ	МАКСИМУМ
1	НЕПРАВИЛЬНАЯ ОБРАБОТКА ПДН	30 000	50 000
2	ОБРАБОТКА БЕЗ СОГЛАСИЯ СУБЪЕКТА	15 000	75 000
3	ОТСУТСТВИЕ ОПУБЛИКОВАННОЙ ПОЛИТИКИ ПДН	15 000	30 000
4	НЕПРЕДОСТАВЛЕНИЕ СУБЪЕКТУ ИНФОРМАЦИИ ОБ ОБРАБОТКЕ	20 000	40 000
5	НЕВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ОБ УНИЧТОЖЕНИИ ПДН	25 000	45 000
6	УТЕЧКА ПДН ИЗ НЕАВТОМАТИЗИРОВАННЫХ СИСТЕМ	25 000	50 000
7	НАРУШЕНИЯ ПРИ ОБЕЗЛИЧИВАНИИ	3 000	6 000
		113 000	**296 000**

Действия по выполнению требований законодательства в области ПДн

1. Определение в каких процессах происходит обработка ПДн
2. Определение состава обрабатываемых сведений
3. Определение правовых оснований обработки ПДн
4. Корректировка состава ПДн в соответствии с целями обработки
5. Определение необходимых сроков обработки ПДн

Перечень документов, разрабатываемых Softline в ходе проектной деятельности

Материалы проектирования	Организационно-распорядительные документы	Эксплуатационные документы
- материалы предпроектного обследования - результаты технического проектирования (материалы разработки и обоснования мероприятий по защите ПДн, описание облика системы защиты ПДн) - результаты опытной эксплуатации и итоговых испытаний	- положения - приказы - должностные инструкции - технические регламенты	- акты, журналы, перечни - инструкции по эксплуатации и правила пользования - формы и соглашения - матрица доступа - описание технологического процесса - протоколы испытаний

Примечание: указанная документация создаёт необходимую основу для осуществления контроля и надзора за обработкой персональных данных со стороны уполномоченных органов (ФСБ, ФСТЭК, Роскомнадзор)

Из чего состоит проект по ПДн

Организационные меры

Разработка документов:

1. Модель угроз, модель нарушителя, акты определения уровня защищенности;
2. Комплекта ОРД (положения, приказы, инструкции);
3. Иные документы по защите персональных данных.

Техническая защита

Применение сертифицированных СрЗИ:

1. Применение СЗИ от несанкционированного доступа;
2. Межсетевые экраны;
3. Защита каналов передачи данных криптографическими средствами;
4. Применение антивируса;
5. Сканер безопасности;
6. Иные СЗИ в зависимости от уровня защищенности ИСПДн.

Основные итоги работы

- Соответствие процессов обработки и обеспечения безопасности ПДн требованиям законодательства РФ
- Минимизация рисков, связанных с проверками регуляторов
- Повышение внутренней дисциплины сотрудников, вовлеченных в процессы обработки ПДн в Компании
- Снижение репутационных рисков для Заказчика, связанных с утечками ПДн

Опыт прохождения проверок Роскомнадзора нашими клиентами

1	Сырьевая компания	Стерлитамак	2012
2	Крупный телеком-оператор	Москва	2015
3	Управляющая жилищная компания	Екатеринбург	2015
4	Краевая больница	Краснодар	2015
5	Государственный ВУЗ	Санкт-Петербург	2015
6	Крупнейшая американская корпорация, производитель в сфере ИТ, аппаратного и программного обеспечения	Москва	2016
7	Крупнейшая французская косметическая компания	Москва	2017
8	Крупнейшая швейцарская корпорация, производитель продуктов питания	Москва	2018
9	Крупнейшая американская корпорация, проихводитель лекарственных препаратов, санитарно-гигиенические товаров и медицинского оборудования	Москва	2018
10	Государственный ВУЗ	Владивосток	2018

Экспресс-аудит ИБ

Cloud | Security | Big Data | Mobility

INFOSECURITY
a Softline company

softline®
25 Years in IT

Что такое экспресс-аудит

Верхнеуровневая оценка состояния ИБ

Основывается на экспертизе, а не комплаенсе

Быстро делается и не отнимает много времени у заказчика

Недорого стоит

В каких случаях нужен?

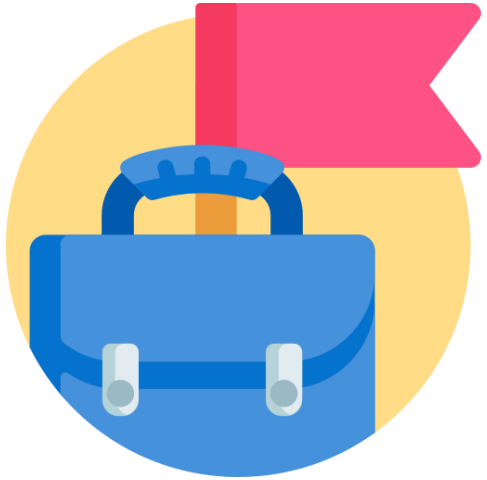
В компании появился новый руководитель по ИБ. Он хочет разобраться в текущем состоянии дел по ИБ

ИБ – нет или им занимается IT-служба. Руководство компании пришло к осознанию, что ИБ необходимо развивать.

Произошел инцидент! С последствиями разобрались*, но компания хочет не допустить повторения и повысить уровень ИБ в целом

** У нас есть также подразделения, занимающиеся расследованием инцидентов ИБ и компьютерных преступлений*

Экспресс-аудит вам поможет



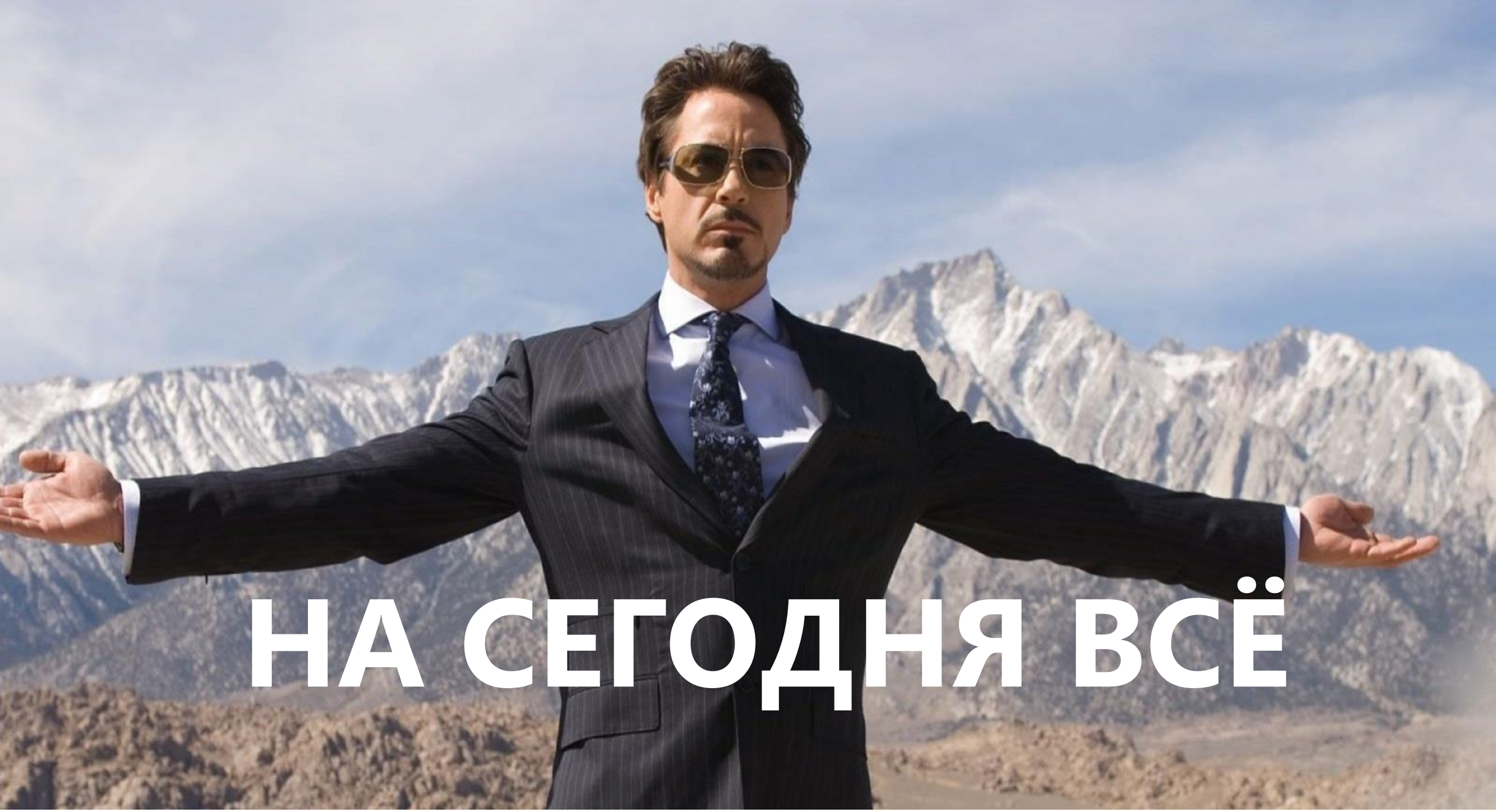
Выяснить уровень текущего состояния процессов ИБ

Определить состав проектов ИБ и необходимые инвестиции

Расставить приоритеты и сформировать план развития ИБ

Обосновать инвестиции в ИБ для руководства

Экспресс-аудит может стать точкой входа в клиента при малых затратах!


НА СЕГОДНЯ ВСЁ