АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Маргарита Дмитриева
Руководитель лаборатории ИБ
Международный институт системных исследований
Преподаватель курсов повышения квалификации

АЛМАТЫ, октябрь 2015

Требования бизнеса сегодня

- Обеспечение требуемого уровня информационной безопасности бизнес-процессов
- Обеспечение требуемого уровня ИТ услуг для обеспечения бизнес-процессов
- Оптимизация операционных затрат
- Снижение капитальных затрат

Требования бизнеса сегодня

- Обеспечение требуемого уровня информационной безопасности бизнес-процессов
- Обеспечение требуемого уровня ИТ услуг для обеспечения бизнес-процессов
- Оптимизация операционных затрат
- Снижение капитальных затрат

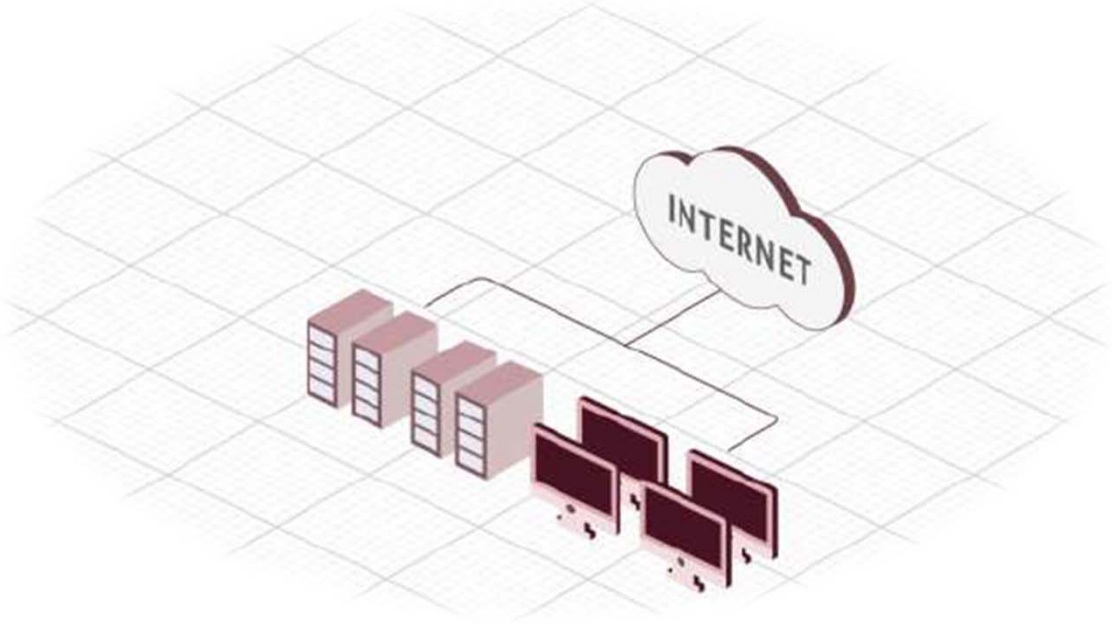
Как следствие - задачи ИБ

- Обеспечение непрерывность работы бизнес-процессов
- Повысить уровень защищенности конфиденциальной информации
- Обеспечить возможность быстрой локализации и устранения последствий инцидентов ИБ
- Снижение затрат на ИБ

Как следствие - задачи ИБ

- Обеспечение непрерывность работы бизнес-процесс
- Повысить уров ень защи енности конфиденци ной инфо ции
- Обеспечить ожност ыстрой локализации и ра последствий инцидентов ИБ
- Снижение затрат на ИБ

В прошлом инфраструктура была проще

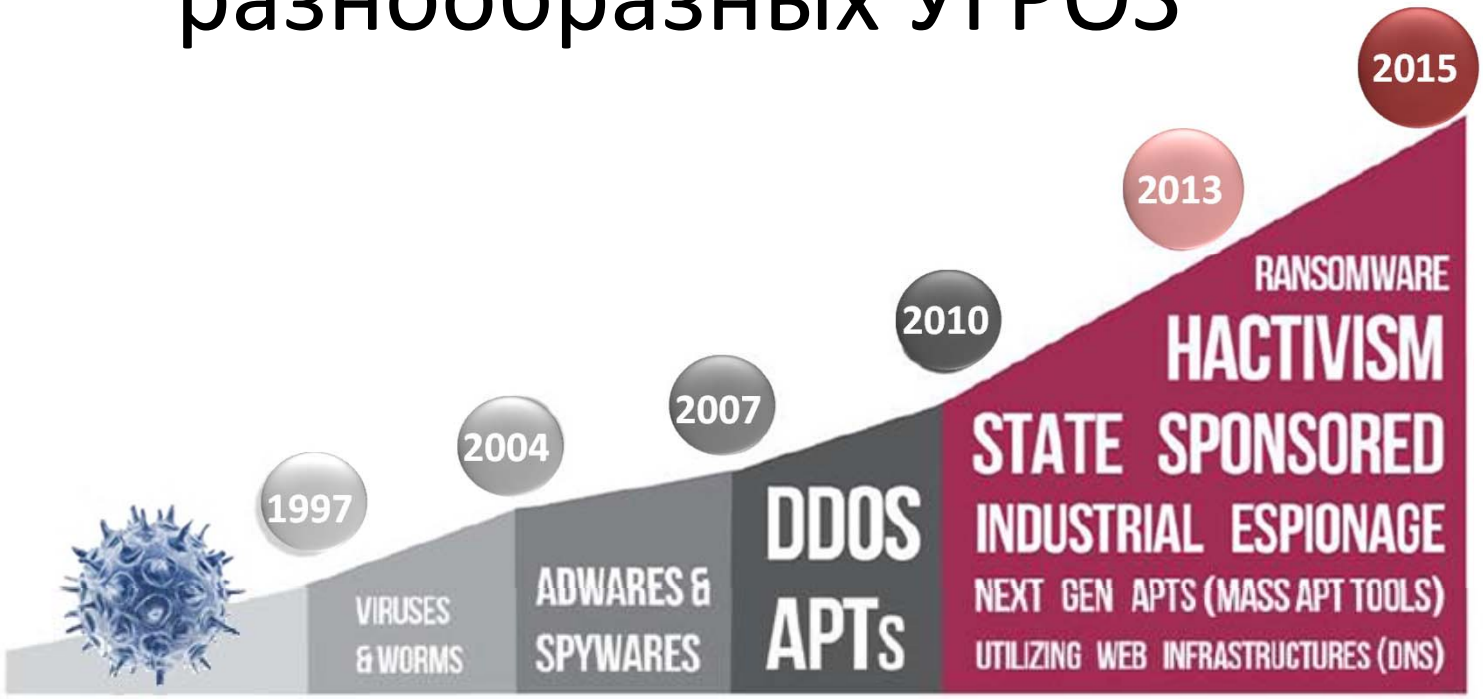


Мы живем во время

повсеместного распространения ТЕХНОЛОГИЙ

Мы живем во время

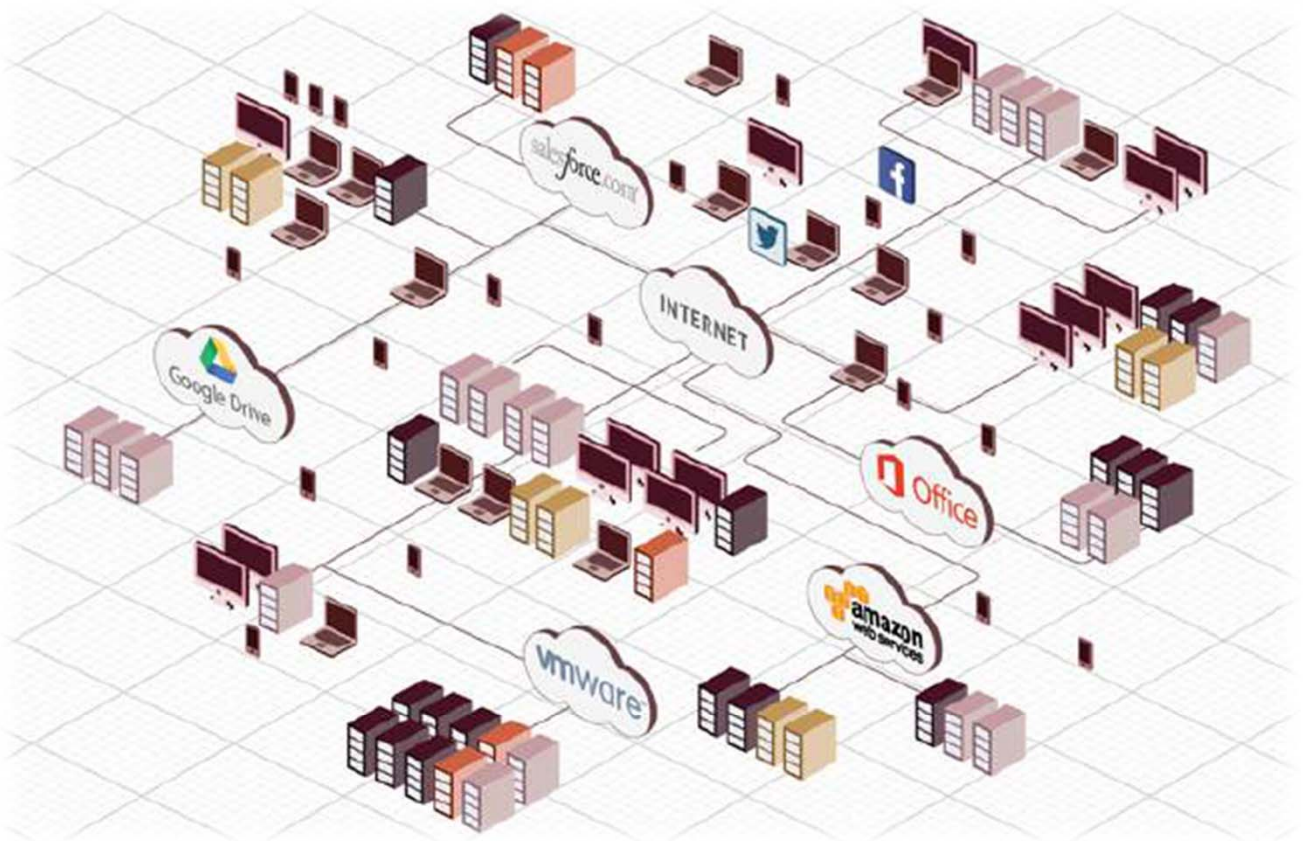
разнообразных УГРОЗ



Мы живем во время когда

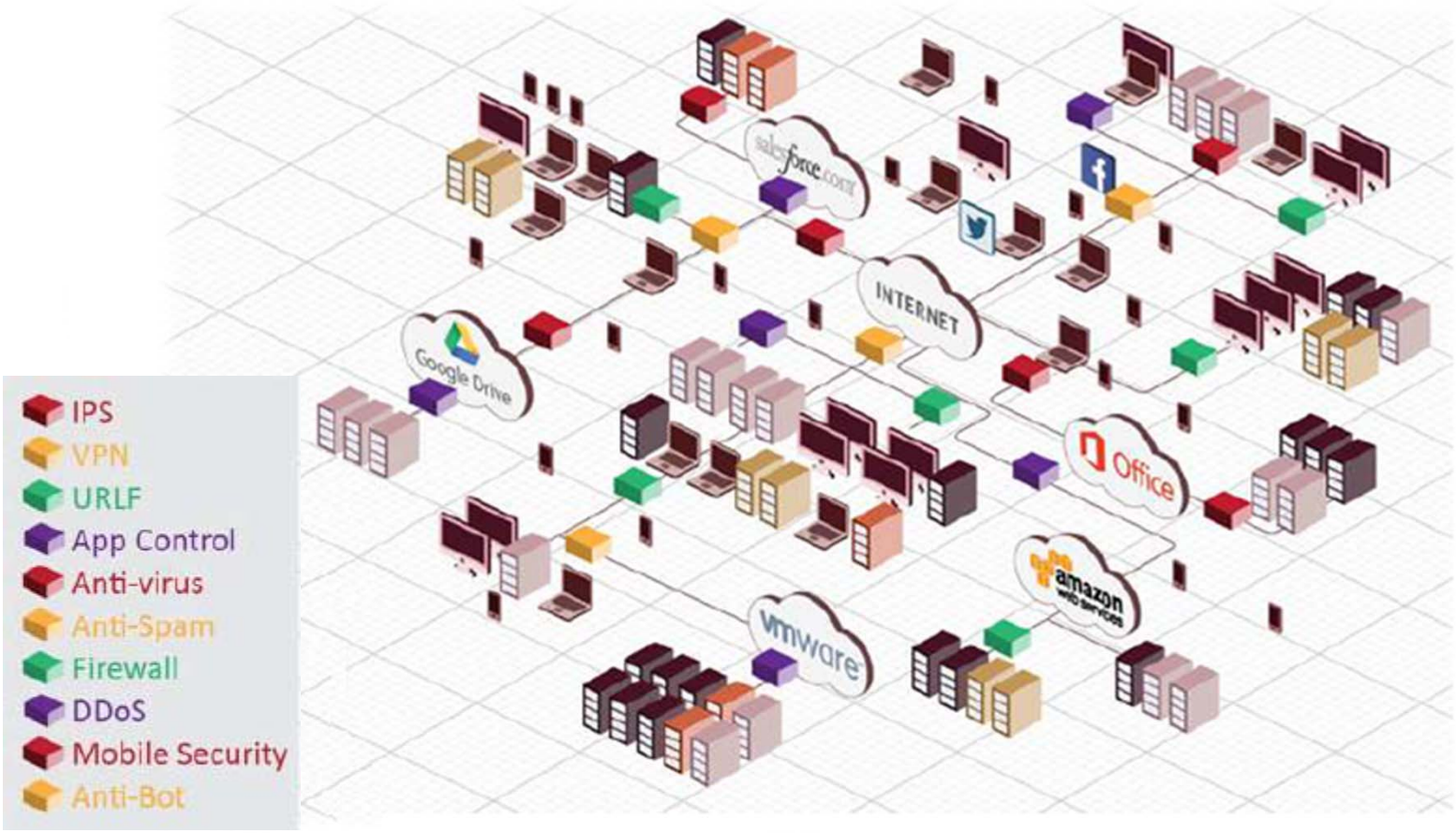
Наблюдается ЗНАЧИТЕЛЬНОЕ изменение IT-архитектуры

Инфраструктура РАЗВИВАЕТСЯ



Как ЗАЩИЩАТЬ инфраструктуру без явных границ

Как ЗАЩИЩАТЬ инфраструктуру без явных границ



Вопросы руководства и бизнеса:

- Может ли наша организация быть целью?
- На какие активы могут быть направлены атаки?
- Где наша инфраструктура уязвима?
- Есть ли риск социальной инженерии или фишинга и как мы можем защититься?
- Можем ли мы защитить все наши активы и инфраструктуру, или мы должны расставить приоритеты на определенные компоненты?
- Как мы можем минимизировать ущерб в случае успешной атаки?

И чем дальше, тем интереснее:

- Эффективны ли наши процессы управления ИБ?
- Лучше ли мы защищены, чем, например, в прошлом году?
- Как мы выглядим в сравнении с конкурентами?
- Сколько мы тратим на ИБ и что получаем взамен?
- Насколько мы соответствуем стандартам или требованиям законодательства?
- Какие наши цели?
- Достигаем ли мы их?
- Оптимально ли мы движемся к поставленным целям?
- Какие средства обработки рисков/средства защиты информации лучше для нас?

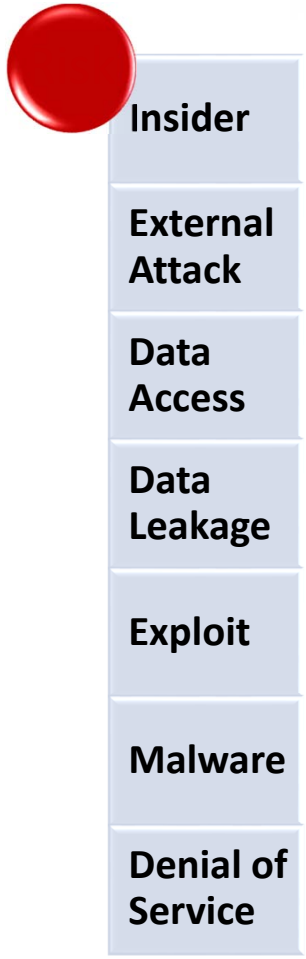
ОРГАНИЗАЦИЯМ НУЖНА
АРХИТЕКТУРА БЕЗОПАСНОСТИ

КОТОРАЯ БУДЕТ

- **МОДУЛЬНОЙ**
- **ГИБКОЙ**
- **ОБЕСПЕЧИВАТЬ ЭФФЕКТИВНУЮ ЗАЩИТУ**

Что же все-таки НЕОБХОДИМО?
И как же УПРАВЛЯТЬ такой инфраструктурой?

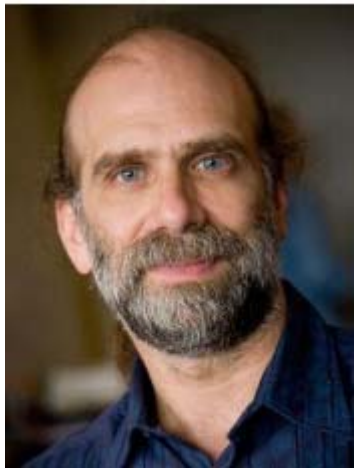
- Оценка рисков
- Классификация данных
- Применение механизмов защиты и политик



На практике это обычно выглядит немного по другому

Категория	Название	Описание	Размещение	Использование (бизнес процессы)	Формат	Конфиденциальность	Целостность	Доступность	Максимальный период недоступности	Сервисы, приложения	Владелец
Веб сайты	Корпоративный сайт Компании	http://компания.ru	офисная сеть	Представительство компании в сети Интернет		_	L	L	1 день		ИТ, маркетинг
	Сайт проекта X	http://проект1.ru	ЦОД	Представительство проекта в сети Интернет, коммуникации с клиентами и партнерами		_	M	M	1 час		ИТ
	Сайт проекта У	http://проект2.ru	ЦОД	Представительство проекта в сети Интернет, коммуникации с клиентами и партнерами		_	L	M	1 час		ИТ
Данные по клиентам и партнерам	Коммерческие предложения		файловый сервер	Работа с клиентами, пресейл	doc	L	_	_	1 неделя		Департамент продаж
	Электронные	Входящая и исходящая электронная почта	файловый	Внутренние и внешние		H	_	M	3 часа		

ID	Задание Сокращения: ДС - Дернов Сергей, РСП - Руководители структурных подразделений	Срок	Ответственный	I квартал 2013 Янв. Фев. Мар.	II квартал 2013 Апр. Май. Июн.	III квартал 2013 Июл. Авг. Сен.
57	5. Внедрение процесса Управления изменениями	180 дней	ААА, ДС			
58	5.1 Проведение аудита процесса приобретения, разработки и поддержки информационных активов	Done	ААА			
59	5.2 Разработка политик и руководств по организации процесса управления изменениями	60 дней	ААА			
60	5.2.1 Политика управления изменениями					
61	5.2.2 Положение о Комитете управления изменениями					
62	5.2.3 Руководство по управлению изменениями					
63	5.2.4 Политика распределения ролей и обязанностей в процессе управления изменениями					
64	5.2.5 Политика приобретения, разработки и поддержки прикладного программного обеспечения					
65	5.3 Утверждение, введение и распространение среди заинтересованных лиц	30 дней	ДС			
66	5.4 Организация ИТ инфраструктуры	90 дней	ИТ			
67	5.4.1 Приобретение сетевого и серверного оборудования для разграничения сред разработки и тестирования					
68	5.4.2 Сегментация сети					
69	5.4.3 Разграничения среды разработки, опытной и промышленной эксплуатации					
70	5.5 Разработка процедур по управлению изменениями	90 дней	ИТ			
71	5.5.1 Процедура внедрения изменений	90 дней	ААА			
72	5.5.2 Процедура внедрения срочных изменений	90 дней	ААА			
73	5.5.3 Процедура опытной эксплуатации изменений	90 дней	ААА			
74	5.5.4 Процедура внедрения релизов	90 дней	ААА			
75	5.5 Утверждение и внедрение процедур по управлению изменениями					
76	6. Организовать процесс безопасной работы с Внешними сторонами	60 дней	ААА, ДС			
77	6.1 Разработать Политику взаимодействия с третьими сторонами	30 дней	ААА			
78	6.2 Разработать Соглашение о конфиденциальности	30 дней	ААА			
79	6.3 Разработать Обязательства "Обязательства о неразглашении работникам третьих Компаний	30 дней	ААА			
80	6.4 Утверждение, введение и распространение среди заинтересованных лиц	30 дней	ДС			



”Безопасность –

это процесс, а не результат.”

- Брюс Шнайер,

Специалист по безопасности, криптограф,

разработчик алгоритма Blowfish

Успех процесса

- Связать стратегию ИБ и цели и потребности компании
- Согласовать долгосрочные цели ИБ
- Использовать в качестве базы оценку и анализ рисков ИБ
- Вовлекать менеджмент
- Постоянно пересматривать СУИБ
- Связать риски ИБ и недостижение компанией своих целей
- Качественная визуализация

Что упускают из вида

- Обучение пользователей
- Поддержка осведомленности
- Обучение персонала ИБ/ИТ
- Поддержка созданной системы

Спасибо за внимание