Методы и средства защиты информации в компьютерных системах

Пермяков Руслан Анатольевич
pra@yandex.ru
@pra_nsk

Литература

- Галатенко В.А. Основы информационной безопасности. – М.:Интуит, 2005
- А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин, А.В.Черемушкин. Основы криптографии (учебное пособие) – М.: Гелиос АРВ, 2004 – 480 с.
- Галатенко В.А. Стандарты безопасности информационных технологий – М.:Интуит, 2006.
- Обеспечение информационной безопасности бизнеса. Под редакцией Курило А.П. Альпина паблишерз 2011г
- Шон Харрис "CISSP All-In-One Exam Guide“ http://dorlov.blogspot.com/2011/05/issp-cissp-all-in-one-exam-guide-pdf.html

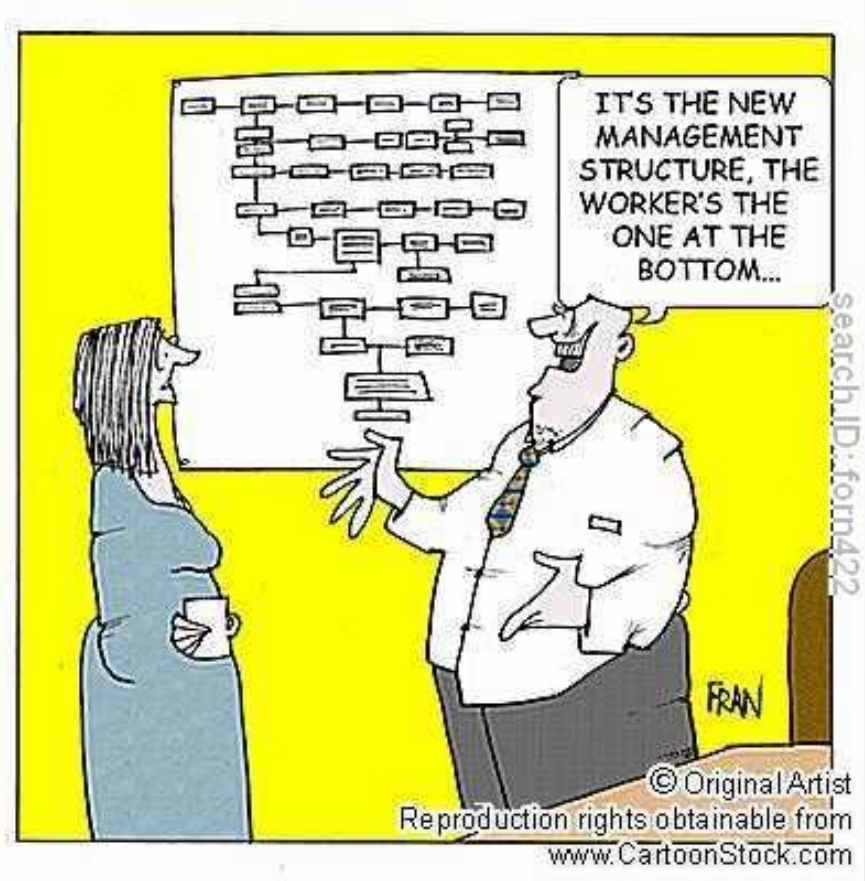
Источники информации

- **Архив ежегодных конференций РусКрипто** http://www.ruscrypto.org/sources/conference/
- www.fstec.ru - Федеральная служба по техническому и экспортному контролю
- www.securitylab.ru - Security Lab by positive technologies
- www.intit.ru - Интернет-Университет Информационных Технологий
- http://wikisec.ru/ - энциклопедия по безопасности информации.

ПОНЯТИЕ БЕЗОПАСНОСТИ БИЗНЕСА

Что такое бизнес?

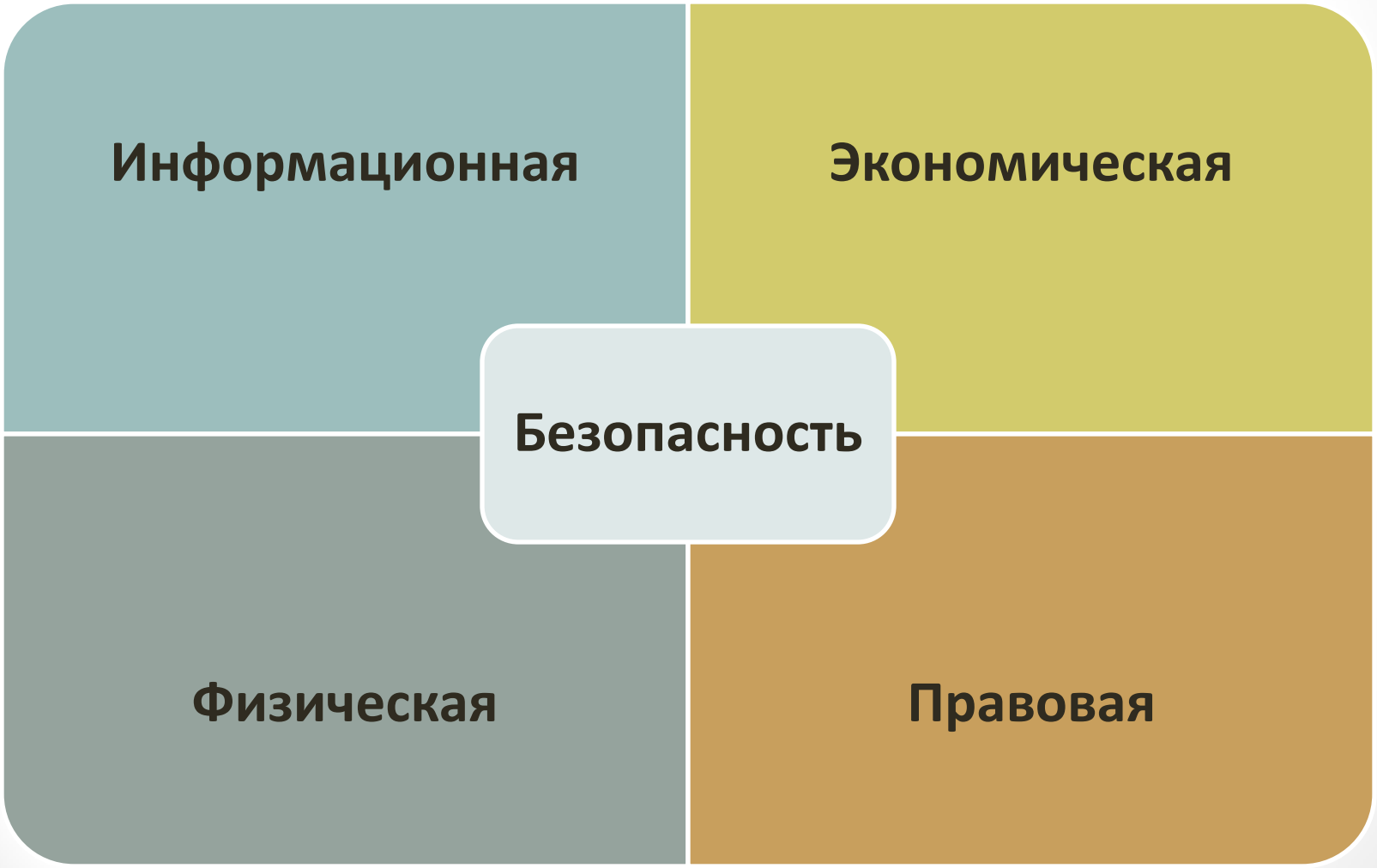
- Know-how
- Бизнес-процесс
- Правовое поле
- Сотрудники
- Партнеры



Бизнес как объект защиты

- Бизнес создается для получения прибыли
- Эффективность бизнеса определяется прибылью который он принес.

Состав понятия безопасности



Определение

- Безопасность (согласно ГОСТ) - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

- Безопасность — такое состояние сложной системы, когда действие внешних и внутренних факторов не приводит к ухудшению системы или к невозможности её функционирования и развития.

Особенности сложных систем

- Наиболее вероятный отклик на единичное воздействие – хаотический
- Обладает новыми свойствами, по сравнению с совокупностью элементов
- Отклик на воздействие не является линейным

Основные свойства безопасности

- Невозможно добиться абсолютной безопасности
- Невозможно измерить уровень безопасности
- Наступление рискового события в общем случае предотвратить невозможно
- Можно понизить степень ущерба, однако, чем реже наступает событие, тем сильнее ущерб
- При любом вмешательстве в систему в первую очередь страдает безопасность

Факторы влияющие на эффективность

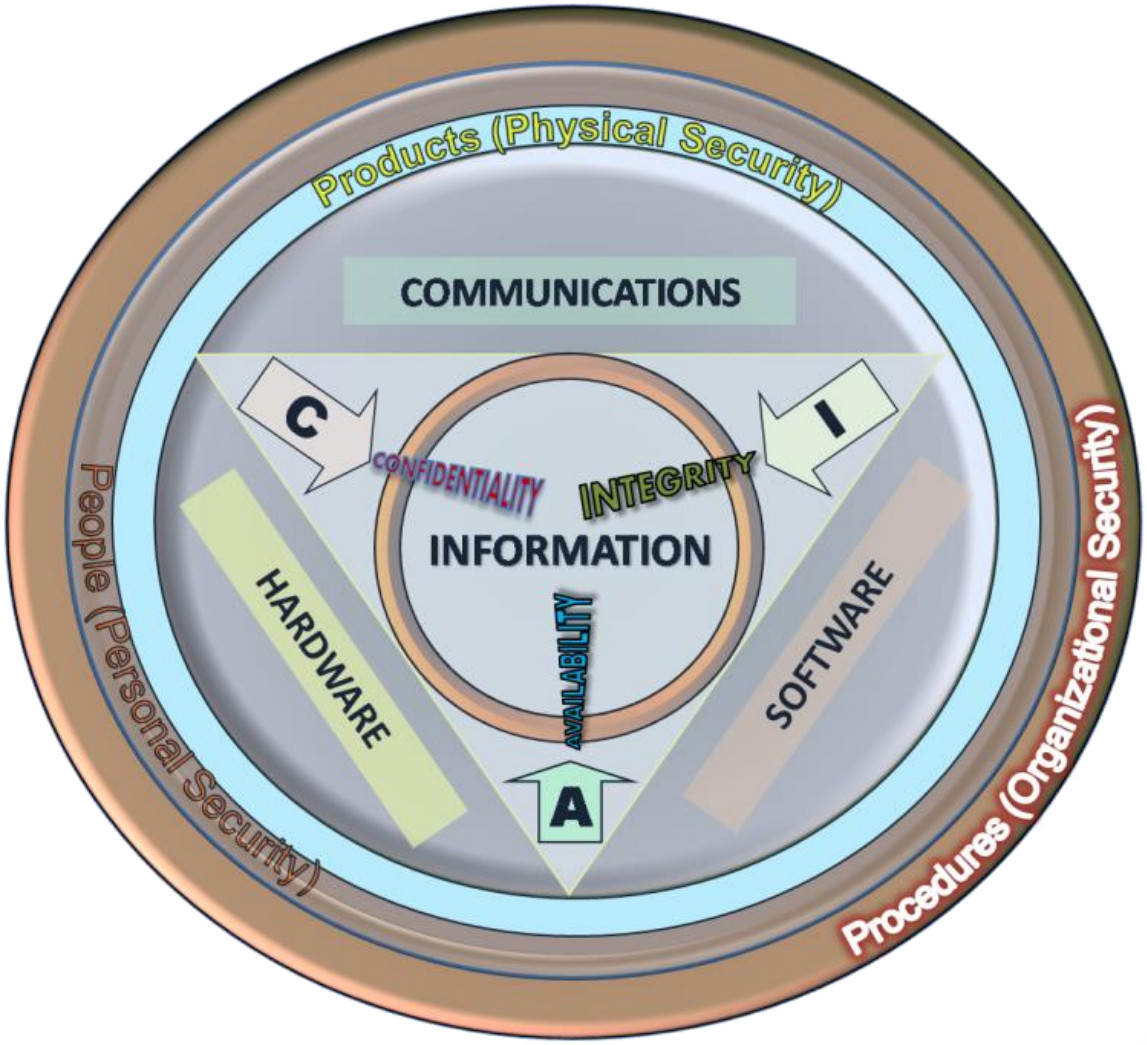
- Величина внутренних издержек (конфликт стоимости СЗИ)
- Качество управления собственным активом (конфликт интересов)
- Качество работы коллектива (конфликт с персоналом)
- Скорость реакции на внешние факторы
- Стратегия и качество ведения самого бизнеса
- Выбранная стратеги управления рисками

Будущее где-то рядом

- Аукцион в электронной форме
- Электронное правительство
- Универсальная электронная карта
- Регламент обмена электронными счетами-фактурами
- Защита персональных данных

ЧТО ТАКОЕ ЗАЩИТА ИНФОРМАЦИИ

Защита информации



Основные задачи ЗИ

- Обеспечение следующих характеристик:
  - Целостность
  - Доступность
  - Конфиденциальность
  - подотчетности;
  - аутентичности;
  - достоверности.

По ГОСТ 13335-4. Методы и средства обеспечения безопасности

Целостность информации

- термин в информатике и теории телекоммуникаций, который означает, что данные полны, условие того, что данные не были изменены при выполнении любой операции над ними, будь то передача, хранение или представление.

Доступность

- **Доступность (информации [ресурсов автоматизированной информационной системы])** (англ.) - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

Конфиденциальность

- свойство, что информация не сделана доступной или не разглашена неуполномоченным лицам, организациям или процессам.

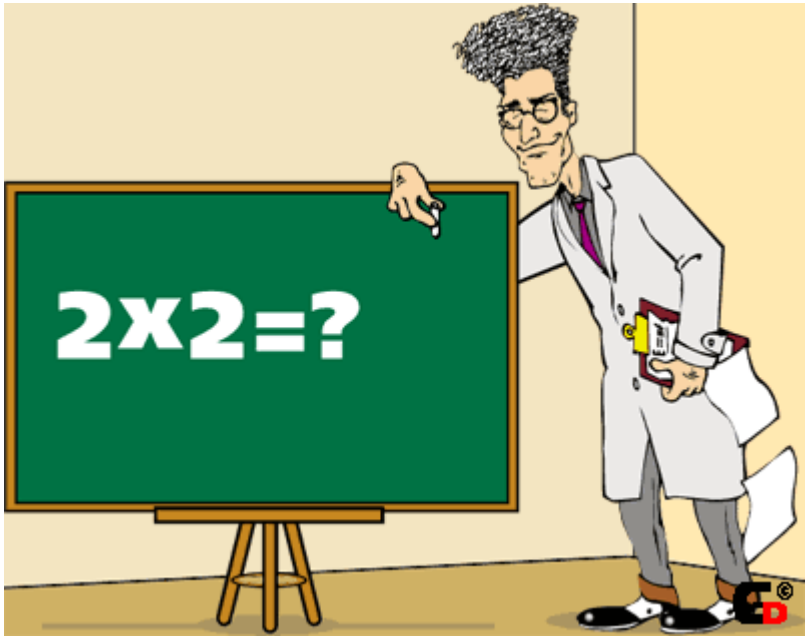
Подотчётность

- **Подотчётность** (англ. accountability) — обеспечение идентификации субъекта доступа и регистрации его действий;

Аутентичность

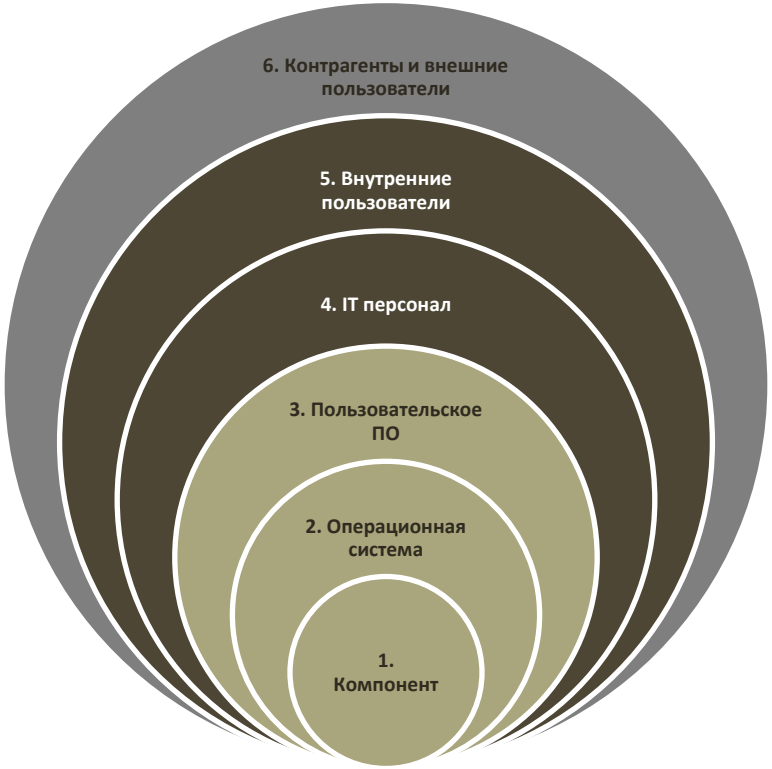
- **аутентичность или подлинность** (англ. authenticity) — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Достоверность



- **достоверность** (англ . reliabilit) — свойство соответствия предусмотренному поведению или результату;

Понятие системы



- Интеграторы имеют в виду 1 или 2 уровень
- Заказчики подразумевают 6 уровень

Доверенный или заслуживающий доверия

Доверенная система

- система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа

Orange Book

Заслуживающая доверия

- Система, в которой можно разместить чувствительные данные и быть уверенным, что они не будут преданы третьим лицам

ПОНЯТИЕ ЗРЕЛОСТИ СОИБ

Уровни зрелости

- 0-й уровень – уровень отсутствия ИБ
- 1-й уровень – частных решений.
- 2-й уровень – уровень комплексных решений
- 3-й уровень – уровень полной интеграции

0-й уровень

- информационной безопасностью в компании никто не занимается, руководство компании не осознает важности проблем информационной безопасности;
- финансирование отсутствует;
- информационной безопасностью реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам).

1-й уровень

- информационная безопасность рассматривается руководством как чисто «техническая» проблема, отсутствует единая программа (концепция информационной безопасности, политика) развития СОИБ компании;
- финансирование ведется в рамках общего ИТ-бюджета;
- информационная безопасность реализуется средствами нулевого уровня плюс средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN (построения виртуальных частных сетей), т.е. традиционные средства защиты.

2-й уровень

- ИБ рассматривается руководством как комплекс организационных и технических мероприятий, существует понимание важности ИБ для бизнес-процессов, есть утвержденная руководством программа развития СОИБ;
- финансирование ведется в рамках отдельного бюджета;
- ИБ реализуется средствами первого уровня плюс средства усиленной аутентификации, средства анализа почтовых сообщений и web-контента, IDS, средства анализа защищенности, SSO (средства однократной аутентификации), PKI (инфраструктура открытых ключей) и организационные меры (внутренний и внешний аудит, анализ риска, политика информационной безопасности, положения, процедуры, регламенты и руководства).

3-й уровень

- ИБ является частью корпоративной культуры, назначен CISA (старший администратор по вопросам обеспечения ИБ);
- финансирование ведется в рамках отдельного бюджета;
- ИБ реализуется средствами второго уровня плюс системы управления информационной безопасностью, CSIRT (группа реагирования на инциденты нарушения информационной безопасности), SLA (соглашение об уровне сервиса).

СОВРЕМЕННЫЕ ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационное окружение

было

- Изолированная ИС
- СУБД
- Офисные пакеты
- Игры
- Вирусы
- Нелегальный контент

стало

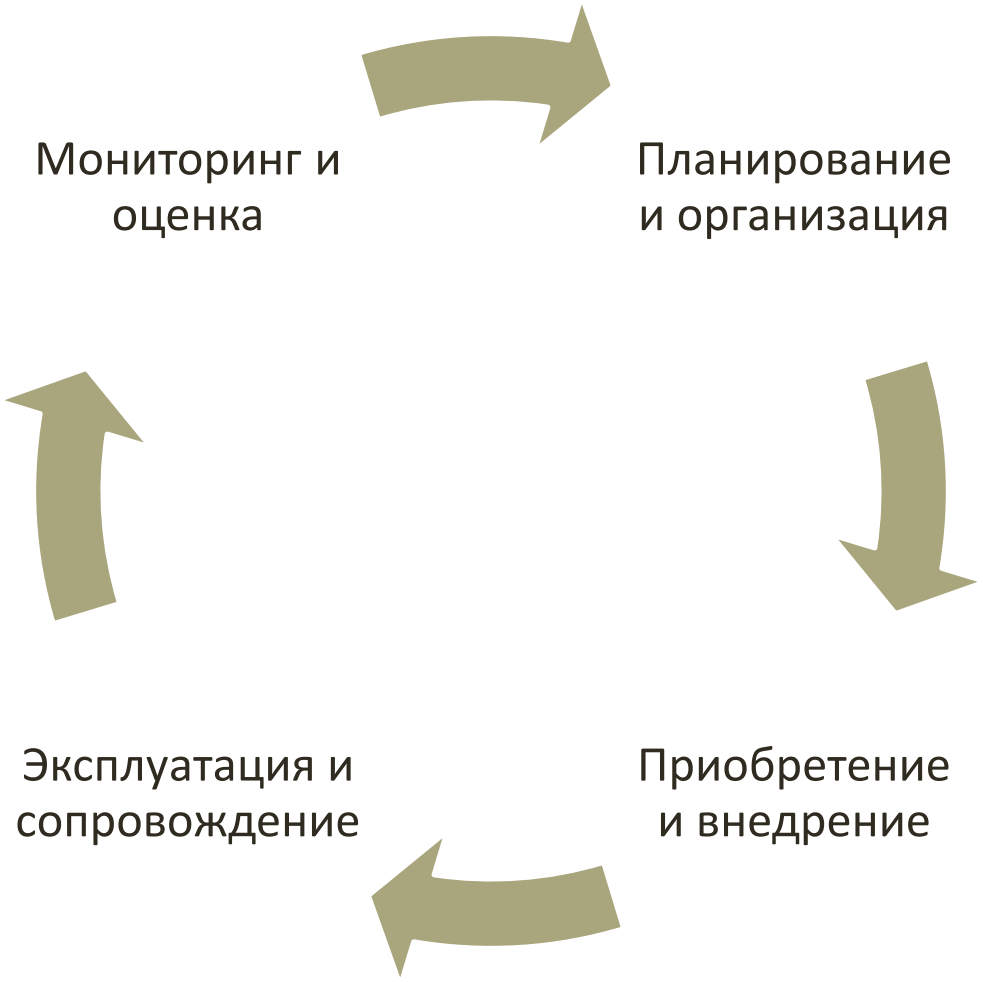
- Облака
- Виртуальные среды
- Web 2.0 (3.0?)
- Социальные сети
- Root Kit
- Advanced Persistent Threat
- StuxNet

Монетизация

- Рассылка spam
- Участие DDOS
- Хранение нелегального контента
- Кража денег

ЖИЗНЕННЫЙ ЦИКЛ ПРОГРАММЫ БЕЗОПАСНОСТИ

Жизненный цикл



Планирование и организация

- Получение одобрения у руководства
- Создание рабочей группы
- Оценка бизнес-драйверов
- Создание профиля угроз
- Проведение оценки рисков
- Разработка архитектурного решения на различных уровнях
  - Организационный
  - Прикладной
  - Сетевой
  - Компонентный
- Фиксация результатов

Приобретение и внедрение

- Распределение ролей и обязанностей в группе
- Разработка
  - Политик безопасности
  - Процедур
  - Стандартов
  - Базисов
  - Руководств и инструкций
- Выявление критичных данных на всех этапах жизненного цикла информации
- Реализация проектов безопасности: Управление рисками, активами, планирование непрерывности бизнеса и д.р.
- Внедрение решений по каждому проекту
- Разработка процедур аудита и мониторинга
- Установка по каждому проекту: метрик, целей, SLA

Эксплуатация и сопровождение

- Соблюдение установленных процедур и базисных уровней в каждом из проектов
- Проведение внутреннего и внешнего аудита
- Выполнение задач в каждом из проектов
- Управление SLA по каждому из проектов

Мониторинг и оценка

- Анализ журналов, результатов аудита, метрик, SLA, по каждому проекту
- Оценка достижений целей по каждому из проектов
- Проведение ежеквартальных встреч рабочей группы
- Совершенствование каждого этапа и возврат на фазу планирования