Расширяющееся пространство: новые возможностей и угроз

Профессор, д.т.н. П. Д. Зегжда
Профессор, д.т.н. Д. П. Зегжда

Санкт-Петербургский государственный политехнический университет

Раздел 1.
Новые технологии: горизонты возможностей

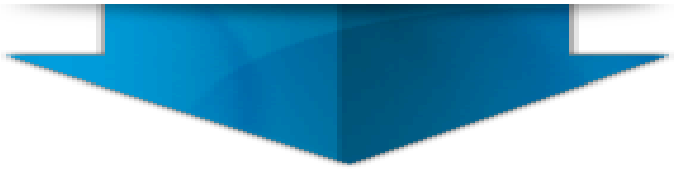
Горизонты технологий

Виртуализация

Облака

Мобильные устройства

«Умный дом»



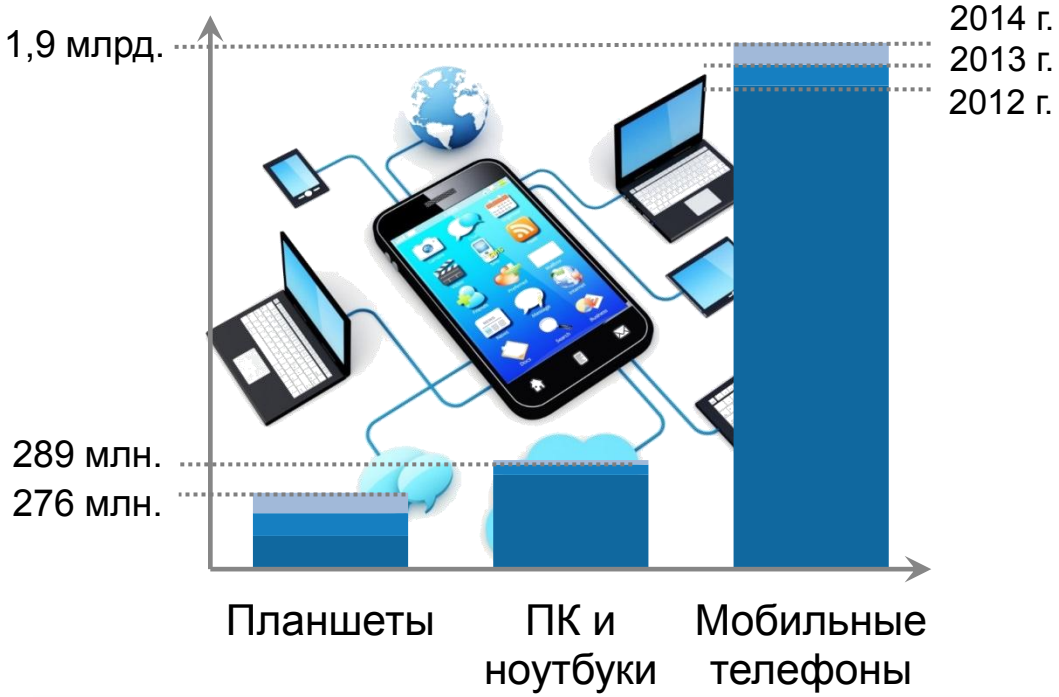
Абсолютная интернетизация общества:

Интернет – универсальная среда, позволяющая с помощью открытых протоколов транзитивно замкнуть все информационные аспекты экономики, политики и частной жизни в единое киберпространство

Мобильные технологии

- Мобильные устройства становятся все более универсальными (голосовая и видеосвязь, просмотр Web-страниц, навигация, электронная почта, редактирование и пересылка документов):

функционально эквивалентны настольным компьютерам, но более распространены



Количество устройств

- Доступ и возможность управления персональными и финансовыми данными (с телефоном всегда связан счет)

Интеллектуальные бытовые устройства: «умный дом»

Элементы «умного дома» – часть глобального киберпространства:
{холодильник, телевизор, пылесос, …} – тоже компьютеры

Определение киберпространства

Киберпространство – глобальная сфера в информационном пространстве, представляющая собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры.

Раздел 2.
Новые технологии: горизонты угроз

Новые горизонты угроз: виртуализация

Кража виртуальных машин

Угрозы ВМ со стороны среды функционирования

Новые горизонты угроз: мобильные устройства

Кроссплатформенное вредоносное программное обеспечение (ВПО)

Прямой доступ к мобильному счету

Новый канал распространения ВПО, не фиксируемый традиционными средствами защиты – перемещение устройства в пространстве

Новые горизонты угроз: «умный дом»

Использование бытовых устройств для проникновения на персональные компьютеры и мобильные телефоны

Угроза жизни и здоровью пользователей (нарушение работы бытовых устройств может привести к пожарам, отравлениям и т.п.)

Подмена медиа-контента в качестве средства ведения информационных войн

Новые горизонты угроз: итог

Новые объекты атаки: данные → инфраструктура → управляющие системы → исполнительные механизмы

Новые цели атаки: перехват управления и навязывание своих алгоритмов управления

Целенаправленный выбор объекта атаки и планирование кибероперaций

Новые механизмы доставки ВПО: от поиска уязвимостей до социальной инженерии

Раздел 3.
Эволюция технологий защиты

Актуальные задачи обеспечения безопасности [1]

- **Быть на шаг впереди в «гонке кибервооружений» и технологий информационной безопасности, выявляя условия появления и реализации киберугроз, тем самым опережая киберпреступность и устраняя благоприятные для них возможности.**

- **Подготовка технических и программных средств для противодействия актуальным и вероятным угрозам.**

- **Проведение мер по обучению персонала и информированию потребителей**

Актуальные задачи обеспечения безопасности [2]

- **Мониторинг и управление безопасностью в распределенных сетях, исследование уязвимостей как новый подход к оценке уровня безопасности.**
- **Интеграция зарубежных информационных технологий и отечественных средств защиты.**
- **Развитие технологии виртуализации как мощного механизма защиты распределенных систем:**
  - **защита собственных средств виртуализации (доверенный гипервизор);**
  - **построение защищенных платформ с использованием технологии виртуализации.**
- **Интеграция средств сетевой защиты и вычислительных кластеров.**
- **Развитие поисковых исследований в части создания моделей политики безопасности систем с размытым периметром и «некорпоративных» систем и средств контроля и управления безопасностью в таких системах.**

Предпосылки появления новой парадигмы информационной безопасности

1. • Рост числа компьютерных атак на системы управления критическими технологиями (Stuxnet, Flame, Duqu, Gauss, Red October, NetTraveler), кражи банковских активов, вывод из строя энергосистем, объектов ядерной промышленности.
2. • Рост эффективности средств разрушающего информационного воздействия как следствие увеличения возможностей информационных систем.
3. • Объектом атаки все чаще становятся не данные, а среда их обработки и системы управления реальными промышленными объектами и инфраструктурой.
4. • Атаки становятся все более тщательно подготовленными, а производство средств их осуществления превратилось в специфическую, но вполне легальную IT-отрасль
5. • Переход от шкалы уровней безопасности к оценке устойчивости систем и определению допустимого риска

Кибербезопасность и новые задачи защиты информации

- Смена объекта защиты: информация (данные) → инфраструктура → управляющие системы → исполнительные механизмы
- Изменение содержания понятий «конфиденциальность», «целостность», «доступность» для систем с открытым периметром и некорпоративных систем
- Разделение среды управления защиты от среды обработки информации
- Необходимость подключения к сети Интернет для обновления ПО
- Новые классификации нарушителей и моделей политик безопасности, переход от доказательной безопасности к допустимому состоянию

ТЕХНОЛОГИЯ ВИРТУАЛИЗАЦИИ – мощнейшее средство защиты, которое позволяет перейти от понятия «защищенная система» к понятию «система с контролируемым поведением»

Эволюция технологий защиты

Характер защиты	Объекты мониторинга			Методы оценки безопасности	Основные характе-ристики
	Состояние системы	Состояние системы защиты	Обмен с окружающей средой		
Статическая	отсутствует	отсутствует	частичный	оценка по нормативным документам	Адекватность угрозам
Активная	частичный	отсутствует	анализ входящей информации	анализ информационной среды	Надёжность анализа входящей информации
Адаптивная	частичный	частичный	анализ входящей информации	контроль состояния средств защиты	Толерантность к угрозам, устойчивость управления
Динамическая	полный	полный	анализ входящей информации и каналов связи	мониторинг безопасности системы, оценка рисков	Инвариантность защиты, достаточность, устойчивость к уязвимостям

Структурная схема системы обеспечения кибербезопасности

Функциональная схема построения систем защиты

Динамическая защита

Мониторинг безопасности

Угрозы

Интернет

Защищаемая система

Статическая защита

Идентификация/ аутентификация

Контроль доступа

Аудит

Обнаружение вторжений

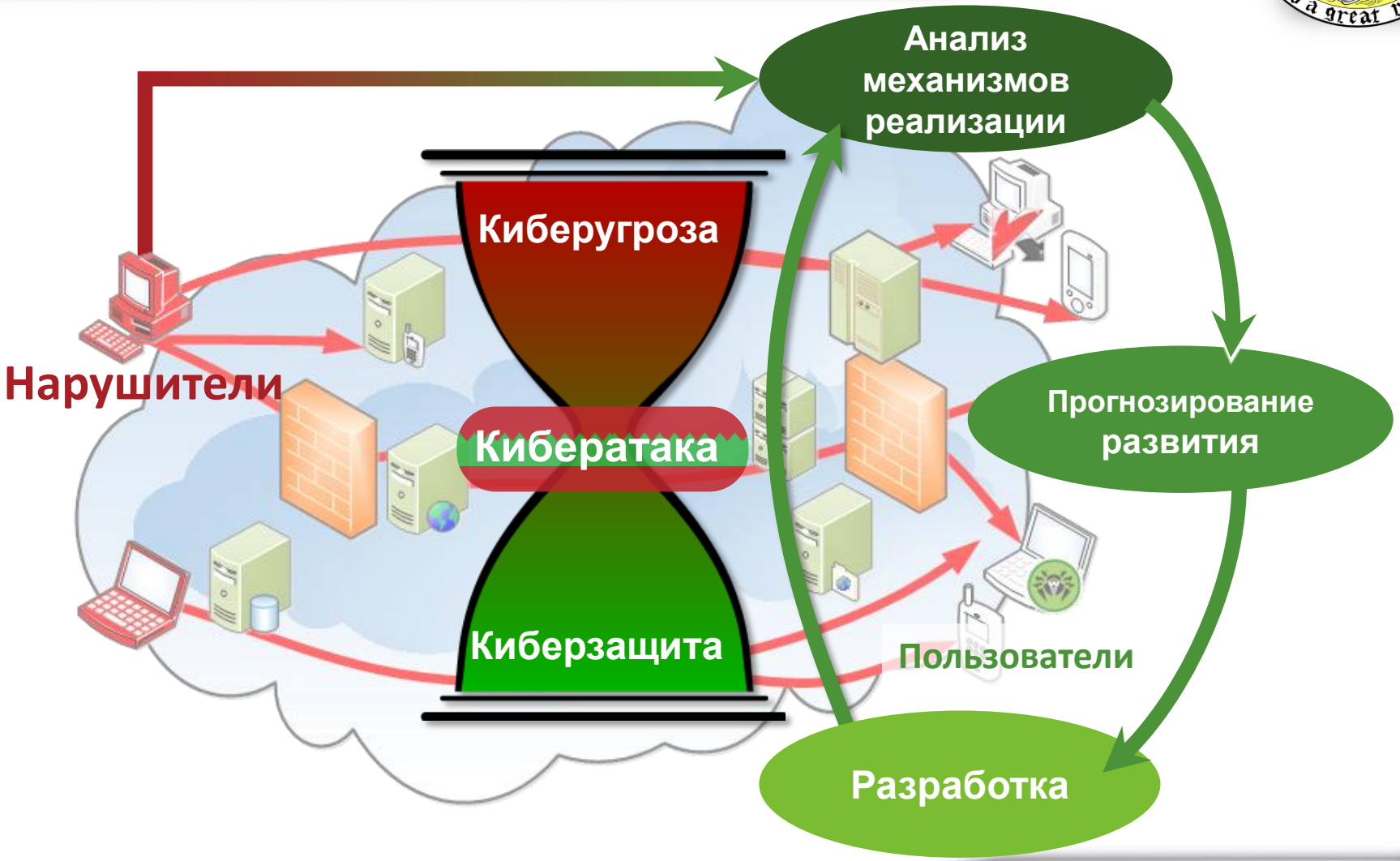
Адаптивная защита

Активная защита

Экспериментальное тестирование защищенности

Подсистема управления кибер-безопасностью

Противодействие киберугрозам



Раздел 4. Кибербезопасность: миф или реальность?

Структура критической информационной среды

Критическая информационная среда

- Субъекты
  - Люди (пользователи, администраторы, операторы систем и т.п.)
  - Абстрактные сущности субъектов (учетные записи, маркеры доступа и т.п.)
- Объекты
  - Компоненты среды передачи информации
    - *Глобальные и локальные компьютерные сети (ЛВС, интранет, Интернет, программно-конфигурируемые сети)*
    - *Мультипротокольное сетевое оборудование(активные коммутаторы, маршрутизаторы)*
    - *Средства коммуникаций (смартфоны, мобильные телефоны, компоненты систем видеоконференцсвязи и т.п.)*
  - Компоненты среды обработки и хранения информации
    - *Мобильные системы*
    - *Операционные системы*
    - *Системы управления базами данных*
    - *Сетевые хранилища данных*
    - *Виртуализированные системы (облака, грид)*
    - *Компоненты их инфраструктуры и поддержки*
  - Компоненты управляющих и технологических систем
    - *Автоматизированные системы управления технологическими процессами (АСУ ТП)*
    - *ERP-системы*
    - *SAP-системы*
    - *Компоненты их инфраструктуры и поддержки*
- Системы защиты
  - Средства защиты
  - Средства управления безопасностью
  - Возможность взаимодействия

Задачи кибербезопасности

Анализ
механизмов нарушения защиты критической информационной среды, моделирование разрушающих воздействий

Управление
кибербезопасностью, определение зоны устойчивости объекта защиты, анализ киберрисков, разработка стандартов и нормативов безопасности критической информационной среды

КИБЕРБЕЗОПАСНОСТЬ

Синтез
средств защиты критической информационной среды, включая ложные цели и активное противодействия

Контроль
текущего состояния компонентов критической информационной среды

В первом приближении *кибербезопасность* трактуется как набор средств и принципов обеспечения безопасности информационных процессов, подходов к управлению безопасностью и прочих технологий, которые используются для защиты критической информационной среды. В этом смысле кибербезопасность не является эквивалентом безопасности данных, безопасности прикладных приложений, сетевой безопасности, Интернет-безопасности и доступности web-сервисов.

Безопасность киберпространства

Не существует **универсальных** средств защиты, так же как и средств реализации угроз, т.к. они **зависимы** от свойств среды функционирования и используемых технологий

Кибербезопасность описывается **игровой** моделью , в которой обе стороны являются активными игроками, проявляющими **инициативу**

Безопасность киберпространства необходимо рассматривать для каждого сегмента по отдельности


cnörny - ubkc - 1997
this is a great mystery