Защита от направленных атак на автоматизированные банковские системы

Назим Латыпаев

nlatypae@cisco.com

Systems Engineer, Cisco EMEAR

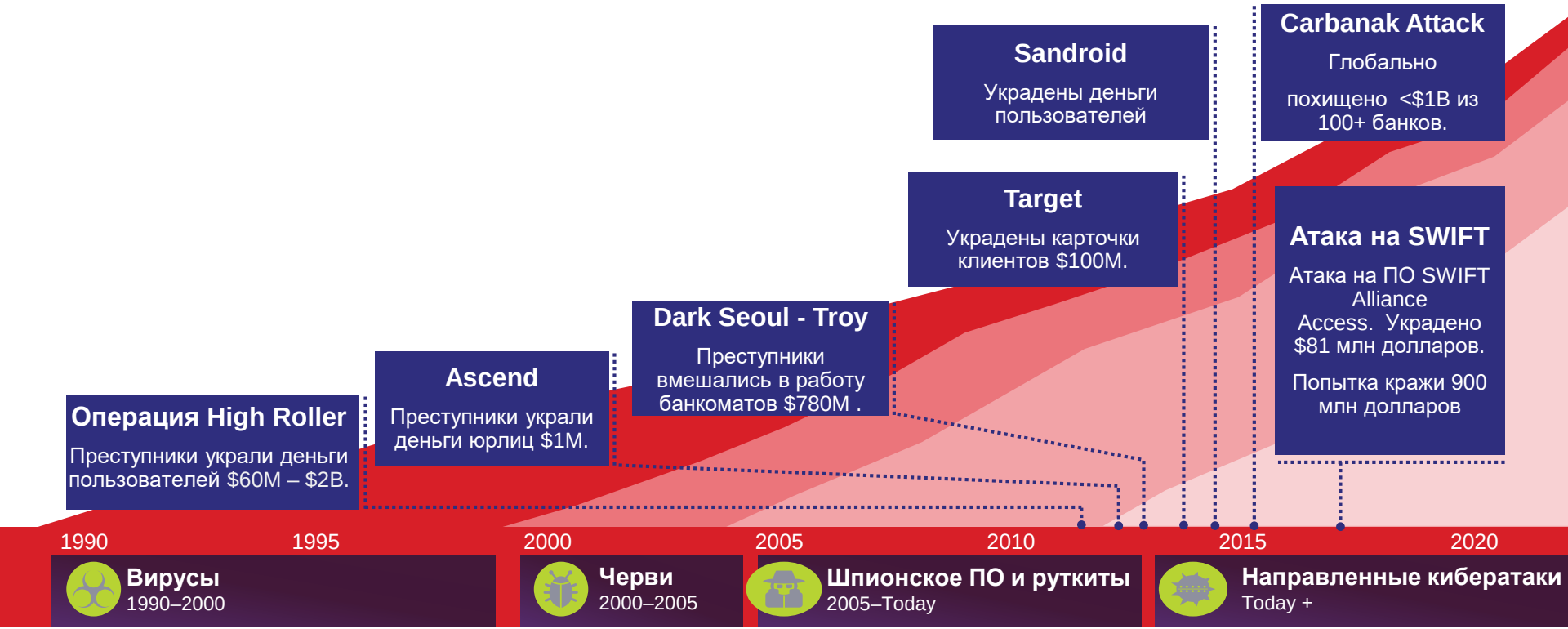
Содержание

- Направление и тенденции
- Нормативы и требования Института финансовой стабильности (FSI) к кибербезопасности
- Решения и технологии компании Cisco
- Ссылки и ресурсы
- Ответы на вопросы

Содержание

- **Направление и тенденции**
- Нормативы и требования Института финансовой стабильности (FSI) к кибербезопасности
- Решения и технологии компании Cisco
- Ссылки и ресурсы
- Ответы на вопросы

Финансовые сервисы под атакой



Краткая история кибератак FSI

- 2008 – 100 миллионов номеров кредитных и дебетовых карт украдено с помощью шпионских программ из платежных систем Heartland
- 2014 – 76 миллионов счетов домохозяйств и 7 миллионов счетов компаний малого и среднего бизнеса были несанкционированно раскрыты в банке JP Morgan Chase
- 2015 - DDoS-атака на финансовую группу OP-Pohjola и банк Danske
- 2016 – атака на Минфин Бангладеш
- ... и еще:
  - Попытка вымогательства в Европейском Центральном Банке
  - Множество банков подверглось атаке Eurograbber

Содержание

- Направление и тенденции
- **Нормативы и требования Института финансовой стабильности (FSI) к кибербезопасности**
- Решения и технологии компании Cisco
- Ссылки и ресурсы
- Ответы на вопросы

Базель III

- Часть 1 включает операционный риск
- Содержит руководство по предотвращению и управлению рисками кибербезопасности, которые рассматриваются как потенциальная опасность для нормального функционирования финансовых учреждений
- Требования к ИТ-безопасности четко НЕ прописаны
- Управление рисками и их контроль - основные элементы и возможность

Стандарт безопасности данных для индустрии платежных карт (PCI DSS)

Стандарт безопасности данных для индустрии платежных карт		
Создание и обслуживание защищенной сети	1. Установить и использовать МСЭ для защиты данных держателя карты 2. Не использовать значения по умолчанию, установленные поставщиком, в качестве системных паролей и других параметров безопасности	✓
Защита данных держателя карты	3. Защищать сохраненные данные держателя карты 4. Шифровать данные держателя карты при передаче их по открытым, публичным сетям	✓
Поддержка программы управления уязвимостями	5. Использовать и регулярно обновлять антивирусное ПО и программы 6. Разработать и поддерживать системы и приложения для обеспечения безопасности	✓
Внедрение действенных мер для контроля доступа	7. Ограничить доступ к данным держателя карты в соответствии с бизнес-потребностями 8. Присвоить уникальный ИД каждому физ. лицу, пользующемуся компьютером 9. Ограничить физический доступ к данным держателя карты	✓
Регулярный контроль и тестирование сетей	10. Отслеживать и контролировать каждый доступ к сетевым ресурсам и данным держателей карт 11. Регулярно тестировать системы и процессы обеспечения безопасности	✓
Выполнение политик информационной безопасности	12. Создать и выполнять политики, включающие требования информационной безопасности для всех сотрудников	✓

- Подход "здравого смысла"
- Обязателен для всех, кто "хранит, обрабатывает или передает данные держателей карт"
- Установлен кредитными организациями
- Затрагивает ритейлеров ("торговые предприятия") и финансовые учреждения ("поставщики услуг")

Европейская служба банковского надзора (EBA)

- Независимая организация ЕС
- Обеспечивает эффективное и согласованное пруденциальное регулирование и надзор для европейского банковского сектора за счет единого свода правил
- Характеризует кибератаки как потенциальный источник риска для нормальной работы учреждений, связанного с ИТ-безопасностью
- Рассматривает кибербезопасность как ответственность финансовых учреждений

Европейское агентство по сетевой и информационной безопасности (ENISA)

enisa
Европейское агентство по сетевой и информационной безопасности

- Агентство по сетевой и информационной безопасности ЕС
- Недавнее начало работы по безопасности FSI
- Предоставляет рекомендации и дорожную карту для определения набора европейских правил (стандартов) для финансовых учреждений
- Сотрудничает с EBA

Содержание

- Направление и тенденции
- Нормативы и требования Института финансовой стабильности (FSI) к кибербезопасности
- **Решения и технологии компании Cisco**
- Ссылки и ресурсы
- Ответы на вопросы

Проблемы в постоянно развивающемся финансовом секторе

Изменение ожиданий клиентов

- Многоканальное взаимодействие
- Персонализация
- Удобство

Переход к цифровым технологиям

- Мобильный банкинг и управление частным капиталом
- Мобильные операторы/претензии
- Мультимедийные коммуникации
- Электронная торговля

Расходы и риски

- Оптимизированные операции и быстрые ИТ-технологии
- Кибербезопасность
- Соответствие нормативным требованиям

Как Cisco реализует концепцию Всеобъемлющего Интернета (IoE) в финансовом секторе?

Совместная работа	Взаимодействие с клиентами на новом уровне Использование высоких технологий для повышения клиентоориентированности
Корпоративные сетевые технологии	Реализация “в любое время” – “в любом месте” Предоставление финансовых услуг
ЦОД/ Виртуализация	Реализация оперативного динамичного применения приложений
Безопасность	Обеспечение безопасной и надежной эксплуатации

>5,9 млрд. долл. США ежегодно тратится на исследования и разработку

Пакет решений Cisco для подключенных банков

Обеспечение многоканального взаимодействия

Центр обработки данных

Полнофункциональный филиал/магазин

Контакт-центры/экспертные центры

Унифицированное рабочее пространство для сотрудников

Централизованная IP-передача голоса и данных для обеспечения унифицированного подключения

Cisco® Remote Expert

Интегрированная система, которая позволяет потребителям динамически связаться с виртуальными экспертами по продуктам и услугам в реальном времени с использованием видеотехнологий совместной работы в HD качестве

Физическая безопасность филиалов

Цифровое видеонаблюдение и аналитика на основе IP для обеспечения безопасности

Технический отсек

Виртуализованное хранение, печать и приложения; беспроводное соединение по каналу 4G LTE

Беспроводные контроллеры и точки доступа

Обеспечение безопасного беспроводного доступа для BYOD, гостевого доступа и персонализированного обращения к клиентам

Контроль окружающей среды

Контроль освещенности и энергопотребления и связь с системой отопления и кондиционирования

Филиал с самообслуживанием

Интерактивный киоск

Самообслуживание, взаимодействие с клиентом, интерактивные вывески и доступ к эксперту

Интерактивные цифровые медиаресурсы

Цифровые вывески для рекламы, бегущие строки, утренние совещания и т.д.

Управление беспроводным банкоматом

Основное или резервное подключение банкомата по каналу 4G LTE

Дома

Cisco Mobile Advisor

Виртуальное решение высокой четкости для контакта с партнерами/поставщиками в любое время

Видео банкомат

Продление рабочих часов банка и предоставление персональных услуг по транзакциям

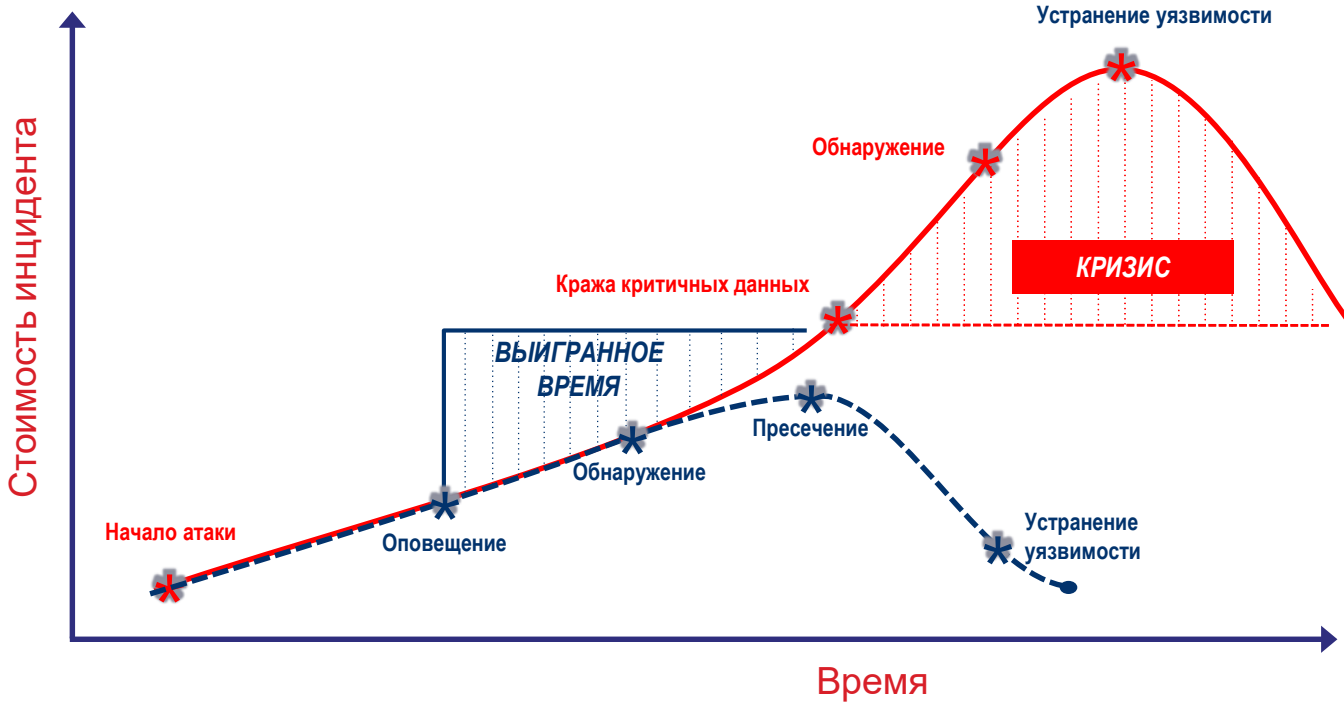
Всеобъемлющая совместная работа

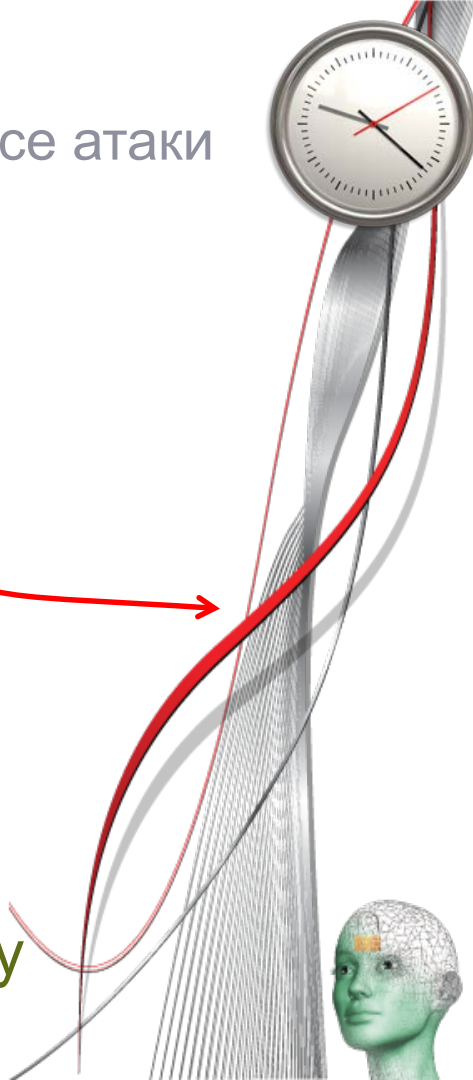
Высококачественная видеосвязь в рамках персонального рабочего пространства

Модель обеспечения безопасности Cisco с ориентацией на предотвращение угроз

Новое измерение – время реагирования

Нельзя устранить все угрозы и на лету остановить все атаки





Задача: выиграть время и устранить причину

Стратегические факторы

Мониторинг

Интеграция в сеть, широкий спектр сенсоров, учет контекста и автоматизация

Ориентация на предотвращение угроз

Постоянно совершенствуемая защита от угроз, средства аналитики в области безопасности на основе облака

На основе платформы

Гибкие, открытые платформы, масштабируемость, согласованный контроль, управление

Сеть

Оконечные устройства

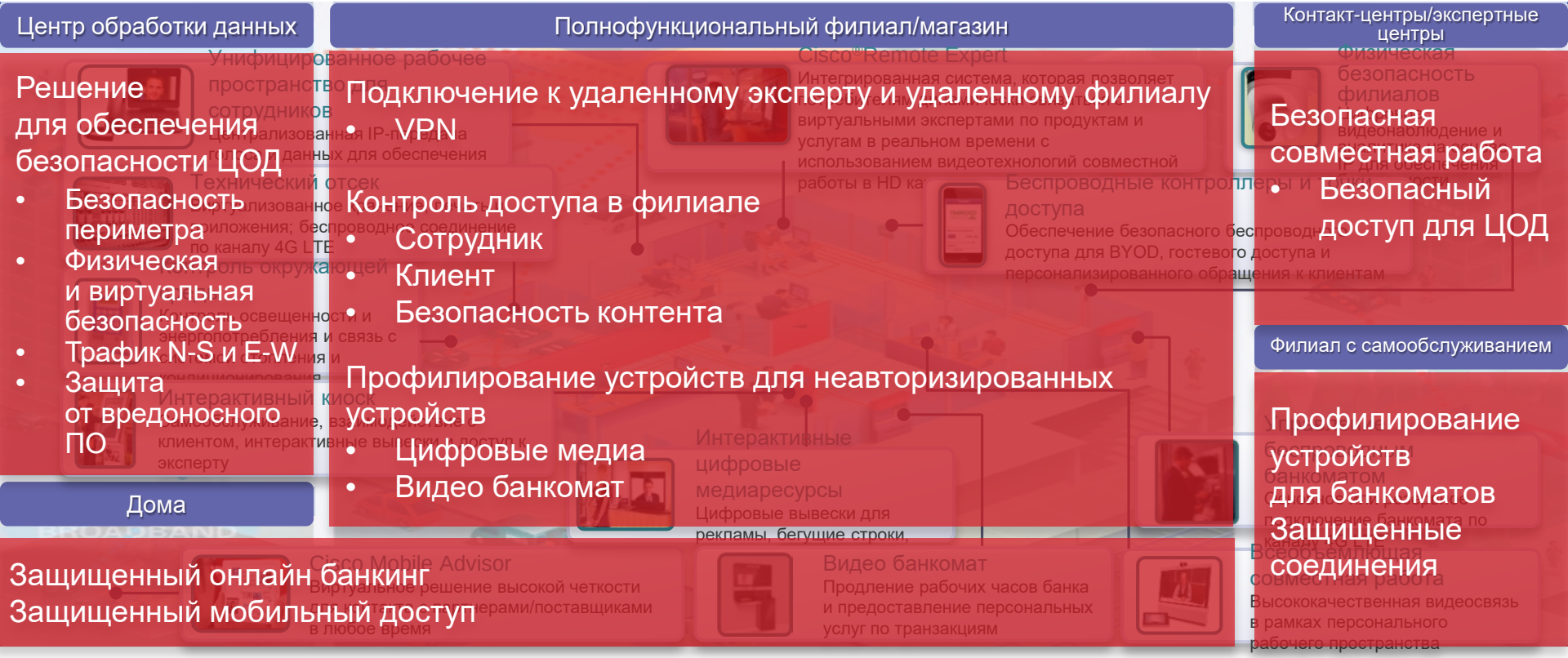
Мобильные устройства

Виртуальные решения

Облако

Пакет решений Cisco для подключенных банков

Обеспечение многоканального взаимодействия



Сервисы безопасности

Консультационные услуги

Пользовательский анализ угроз

Техническая оценка безопасности

Интеграция

Услуги по интеграции

Услуги по оптимизации безопасности

Управляемые услуги

Управляемая защита от угроз

Удаленные управляемые услуги

Команды, предоставляющие услуги Cisco в области безопасности по разным направлениям

	Финансовые услуги	Операторы связи	Управление и SCADA-система	Корпорации и предприятия
Красный	• Выполняется красной командой • Тестирование проникновения (SPA) • Расширенные постоянные угрозы (APT)		• Фишинговые кампании • Физическое проникновение	
Синий	• Оценка дизайна системы безопасности • Дизайн SOC • Сегментация сети		• Безопасность и оптимизация E2E • Безопасность облачной среды • Безопасность SDN	
Белый	• Услуга поддержки управления • Оценка рисков • Военные игры		• Программа управления уязвимостями	

Содержание

- Направление и тенденции
- Нормативы и требования Института финансовой стабильности (FSI) к кибербезопасности
- Решения и технологии компании Cisco
- **Ссылки и ресурсы**
- Ответы на вопросы

Дополнительная информация

- Европейская служба банковского надзора (EBA) - http://www.eba.europa.eu
- Европейское агентство по сетевой и информационной безопасности (ENISA) - http://www.enisa.europa.eu
- Базель III - http://www.basel-iii-accord.com/
- Стандарт безопасности данных для индустрии платежных карт (PCI DSS) - https://www.pcisecuritystandards.org/
- Архитектура и руководство по внедрению решений Cisco для соответствия требованиям PCI DSS

  http://www.cisco.com/c/en/us/solutions/enterprise-networks/pci-compliance/index.html

Только с помощью решений Cisco!

Непревзойденный мониторинг

Широкие аналитические возможности благодаря правильному контексту

Постоянный контроль

Согласованные политики в масштабе сети и ЦОД

Усовершенствованная защита от угроз

Обнаружение и блокирование новейших угроз

Уменьшение сложности

Полная интеграция и адаптация к меняющимся бизнес-моделям

Благодарю за внимание