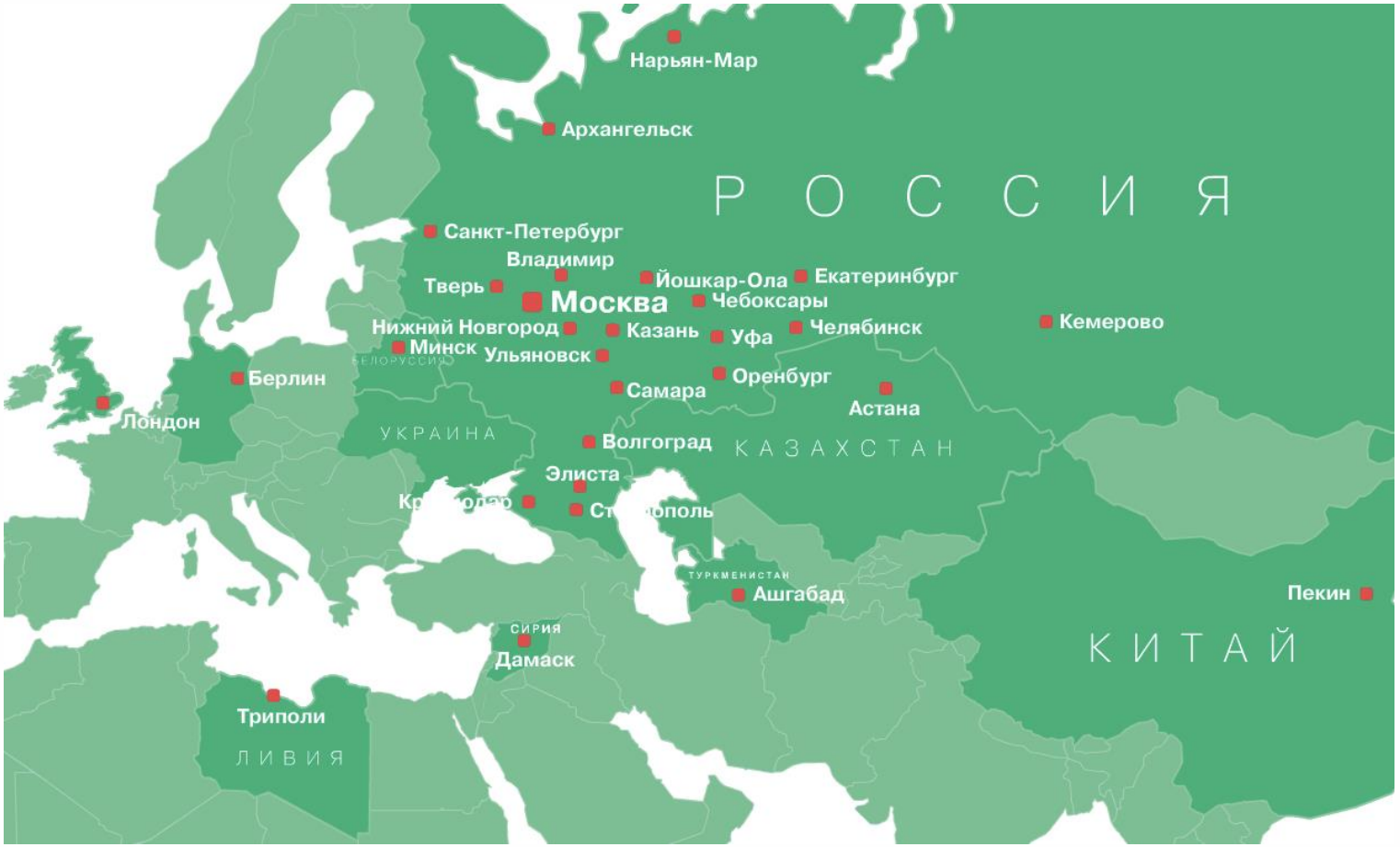
Концепция
информационной безопасности

Докладчик:
Камалетдинов Артур Рафаэлевич

СОДЕРЖАНИЕ

3 ТЕКУЩЕЕ СОСТОЯНИЕ



~30 регионов присутствия

ТЕКУЩЕЕ СОСТОЯНИЕ

Структура Группы

~70 подразделений, часть из которых имеет независимую ИТ политику, что представляет еще большую угрозу ИТ безопасности.

ПРОБЛЕМА

- Вопросы информационной безопасности:
  - Государственные и проверяющие органы;
  - Сотрудники – невнимательность и халатность;
  - Программное обеспечение – не лицензионное ПО, не своевременное обновление;
  - Атаки из вне – получение доступа из вне, использование ресурсов, нарушение работоспособности;
  - Вирусная активность – вымогательство, подготовка для атак из вне;
  - Привилегированные пользователи – нарушители, преступники, кроты, обиженные;

ПРОБЛЕМА

- Государственные и проверяющие органы:
  - Угроза:
    - Имеют право конфисковать и вывозить оборудование и носители информации;
  - Последствия:
    - Остановка деятельности подразделения;
    - Потеря информации;
    - Нарушение целостности информации;
    - Раскрытие информации;
    - Заражение носителей информации вирусами;
    - Закладки для доступа из вне.

ПРОБЛЕМА

- Государственные и проверяющие органы:
  - Угроза:
    - ФЗ № 152 – «О персональных данных»;
  - Последствия:
    - Уголовная ответственность до 4-х лет;
    - Административная ответственность;
    - Гражданско-правовая ответственность;
    - Репутационные риски.

ПРОБЛЕМА

- Государственные и проверяющие органы:
  - Угроза:
    - ФЗ № 187 – «О безопасности критической информационной инфраструктуры Российской Федерации»;
  - Последствия:
    - Уголовная ответственность до 10 лет;
    - Административная ответственность;
    - Гражданско-правовая ответственность;
    - Репутационные риски.

ПРОБЛЕМА

- Сотрудники (лояльные и не злонамеренные, но халатные и не внимательные) :
  - Угроза:
    - Социальная инженерия (фишинг, зараженные письма и т.п.);
    - Вынос информации за периметр (забыл документы, оставил флешку, отправил не по тому адресу, утеря пропусков и ключей доступа);
  - Последствия:
    - Раскрытие информации;
    - Заражение вирусами;
    - Предоставление доступа из вне;

ПРОБЛЕМА

- Программное обеспечение:
  - Угроза:
    - Не лицензионное ПО;
  - Последствия:
    - Претензии со стороны правообладателя;
    - Заражение вирусами;
    - Предоставление доступа из вне;
    - Не стабильная работа;
    - Потеря информации;
    - Искажение информации.

ПРОБЛЕМА

- Программное обеспечение:
  - Угроза:
    - Не своевременное обновление ПО;
  - Последствия:
    - Заражение вирусами;
    - Предоставление доступа из вне;
    - Не стабильная работа;
    - Потеря информации;
    - Искажение информации.

ПРОБЛЕМА

- Атаки из вне:
  - Угроза:
    - Сторонние пользователи тем или иным способом получают доступ к ресурсам из вне;
  - Последствия:
    - Остановка деятельности подразделения;
    - Вывод из строя оборудования;
    - Нарушение технологических процессов;
    - Потеря информации;
    - Нарушение целостности информации;
    - Раскрытие информации;
    - Хищение;
    - Вымогательство;
    - Шантаж.

ПРОБЛЕМА

- Вирусная активность :
  - Угроза:
    - Злонамеренное или нет заражение ресурсов компьютерными вирусами;
  - Последствия:
    - Остановка деятельности подразделения;
    - Вывод из строя оборудования;
    - Нарушение технологических процессов;
    - Потеря информации;
    - Нарушение целостности информации;
    - Раскрытие информации;
    - Хищение;
    - Вымогательство;
    - Шантаж.

ПРОБЛЕМА

- Привилегированные пользователи :
  - Угроза:
    - Нарушители – используют расширенные права для использования ресурсов компании в личных целях;
  - Последствия:
    - Потеря информации;
    - Нарушение целостности информации;
    - Раскрытие информации;
    - Вирусная активность;
    - Предоставление доступа из вне.

ПРОБЛЕМА

- Привилегированные пользователи :
  - Угроза:
    - Преступники – осознанно используют расширенные права для передачи внутренней информации за пределы периметра;
  - Последствия:
    - Раскрытие информации;
    - Заражение вирусами;
    - Предоставление доступа из вне.

ПРОБЛЕМА

- Привилегированные пользователи :
  - Угроза:
    - Кроты – осознанно и за вознаграждение используют расширенные права для передачи внутренней информации за пределы периметра;
  - Последствия:
    - Раскрытие информации;
    - Заражение вирусами;
    - Предоставление доступа из вне.

ПРОБЛЕМА

- Привилегированные пользователи :
  - Угроза:
    - Уволенные и обиженные сотрудники – осознанно используют расширенные права для реализации угроз ИБ;
  - Последствия:
    - Остановка деятельности подразделения;
    - Вывод из строя оборудования;
    - Нарушение технологических процессов;
    - Потеря информации;
    - Нарушение целостности информации;
    - Раскрытие информации;
    - Хищение;
    - Вымогательство;
    - Шантаж.

ПРОБЛЕМА

- Элементы информационной безопасности присутствуют:
  - Антивирусы;
  - Межсетевые экраны;
  - Организационно-распорядительные документы;
- И вместе с тем, стоит учесть частое отсутствие единой системы информационной безопасности, что позволяет реализовать вышеописанные угрозы.

РЕШЕНИЕ

- 11 уровневая модель ИТ
  - Уровень международных стандартов;
  - Уровень законодательства;
  - Уровень бизнеса;
  - Уровень пользователей;
  - Уровень АРМ пользователей;
  - Уровень конфигурации серверов;
  - Уровень серверов;
  - Уровень операционных систем;
  - Уровень конфигурации аппаратных средств;
  - Уровень физического расположения;
  - Уровень инфраструктуры.

РЕШЕНИЕ

- Уровень международных стандартов, на этом уровне описываются требования международных стандартов к бизнесу в области ИТ:
  - ГОСТ Р ИСО/МЭК 20000 «Информационная технология. Менеджмент услуг»;
  - ГОСТ Р ИСО/МЭК 27000 "Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности...».

РЕШЕНИЕ

- Уровень законодательства, на этом уровне описываются требования государственных структур к бизнесу в области ИТ:
  - ФЗ №152, Персональные данные;
  - ФЗ №187, О безопасности критической информационной инфраструктуры;
  - Прочие законодательные акты.

РЕШЕНИЕ

- Уровень бизнеса, на этом уровне описываются требования бизнеса к ИТ, в формализованном виде (положения, стандарты и т.п.), что зачем и как бизнес хочет от ИТ:
  - Непрерывность;
  - Масштабируемость по размеру и скорости;
  - Управление различными видами рисков, в т. ч. информационной безопасности;
  - Управляемости ИТ;
  - Стоимость владения.

РЕШЕНИЕ

- Уровень пользователей, на этом уровне описываются требования различных групп пользователей к ИТ ресурсам и сервисам:
  - Необходимые знания, навыки и умения при работе с прикладными решениями.
  - Информационная безопасность;
  - Охрана труда.

РЕШЕНИЕ

- Уровень АРМ пользователей, на этом уровне описывается что, как и зачем предоставляется пользователю:
  - Аппаратные средства - ПЭВМ, принтер, сканер, мобильный телефон, планшет и т.п. Порядок, скорость обслуживания. Периоды ТО и т.п.
  - Операционная система пользователя. Обновление, унификация и т п.
  - Базовые сервисы, предоставляемые локально - офис, антивирус.
  - Сетевые сервисы пользователя - почта, 1С, портал, lync.

РЕШЕНИЕ

- Уровень конфигурации серверов*, на этом уровне описывается, как и зачем каждый сервер сконфигурирован, как кому и зачем предоставляет свои ресурсы. Данный уровень включает в себя сервисы обслуживания конфигураций серверов:
  - Сервис конфигурации серверов. Какая конфигурация установлена, как кем и кто имеет доступ. Периоды обслуживания и обновления.
  - Сервис интеграции серверов. Как кому и зачем предоставляются ресурсы, кто обслуживает, поддерживает и обеспечивает.

* «Сервер - программный компонент вычислительной системы, выполняющий сервисные (обслуживающие) функции по запросу клиента, предоставляя ему доступ к определённым ресурсам или услугам»

РЕШЕНИЕ

- Уровень серверов, на этом уровне описывается где, как и зачем какой сервер установлен. На этом уровне находятся сервисы обслуживания серверов:
  - Сервис программного сервера. Какой сервер установлен, как обслуживается кем и когда, период и способ обновлений, кто имеет доступ.

РЕШЕНИЕ

- Уровень операционных систем, на этом уровне описывается какая операционная система где и зачем установлена. На этом уровне находятся сервисы обслуживания операционных систем:
  - Сервис операционная система аппаратного элемента. Какая операционная система установлена, как обслуживается кем и когда, период и способ обновлений, кто имеет доступ.

РЕШЕНИЕ

- Уровень конфигурации аппаратных средств, на этом уровне находятся сервисы обеспечивающие физическую связь между аппаратными элементами:
  - Сервис физической коммутации. Что с чем, как и почему связано. Кто имеет доступ, кто обслуживает, когда и зачем.

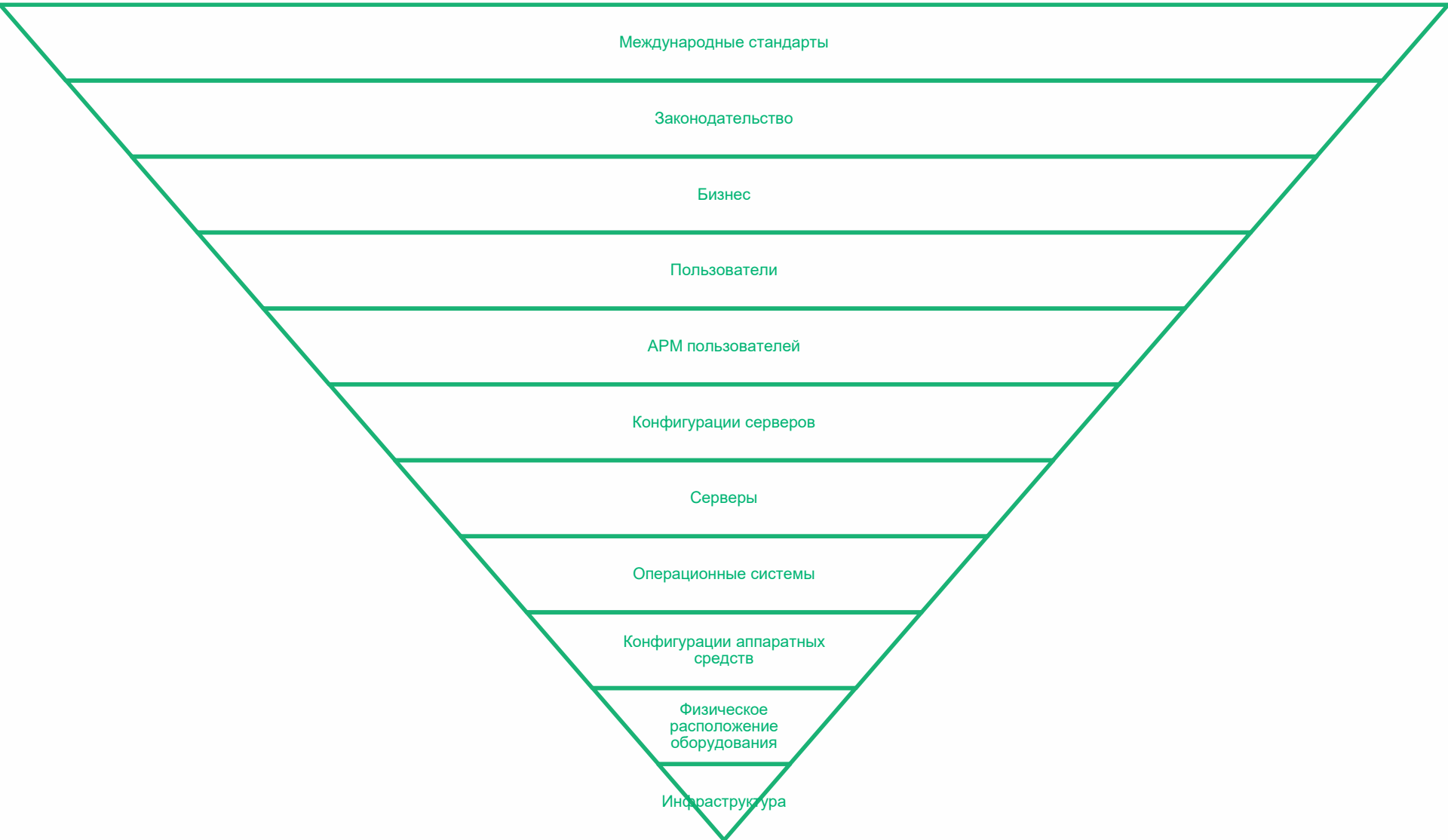
РЕШЕНИЕ

- Уровень физического расположения, на этом уровне описывается физическое размещение ИТ аппаратных средств т. е., что где и как расположено. На данном уровне находятся сервисы обеспечивающие физическое размещение ИТ оборудования, как-то:
  - Сервис размещения аппаратного элемента (сервера, схд, коммутатора и т и т п) в стойке. Какое оборудование, в какой стойке расположено, какое электропитание подведено, сколько электропитания, кто, когда как и зачем обслуживает (чистит, моет, продувает), имеет доступ, перемещает.

РЕШЕНИЕ

- Уровень инфраструктуры, этот уровень описывает не ИТ сервисы, присутствующие в ИТ инфраструктуре. На данном уровне находятся сервисы обеспечивающие физическое функционирование ИТ инфраструктуры, как-то:
  - Подуровень Центр обработки данных;
  - Подуровень Узлы связи;
  - Подуровень Обособленный коммутационный шкаф, для подразделений, не имеющих ни узла связи ни ЦОД.

РЕШЕНИЕ


Международные стандарты
Законодательство
Бизнес
Пользователи
АРМ пользователей
Конфигурации серверов
Серверы
Операционные системы
Конфигурации аппаратных средств
Физическое расположение оборудования
Инфраструктура

РЕШЕНИЕ

- Мероприятия по созданию системы обеспечения ИБ :
  - Провести обследование по каждому уровню ИТ инфраструктуры с точки зрения ИБ и учетом идущих проектов.
  - Выработать решения и подготовить ТЗ.
  - Запроектировать выработанные решения.
  - Реализовать выработанные решения.
  - Сопровождение - обслуживание, поддержание работоспособности и мониторинг.

РЕШЕНИЕ

- Система обеспечения ИБ
  - Система обеспечения информационной безопасности (СОИБ) - комплексное решение, позволяющее определять актуальные угрозы и уязвимость информационной безопасности и надлежащим образом организовывать защиту.
  - Задачи:
    - Защита объектов информационной системы;
    - Защита процессов, процедур и программ обработки информации;
    - Защита каналов связи;
    - Управление системой защиты.

РЕШЕНИЕ

- Обследование
  - Цель:
    - Выявление рисков информационной безопасности на каждом уровне ИТ инфраструктуры
  - Задачи:
    - Определение информационных и технических ресурсов, подлежащих защите;
    - Выявление полного множества потенциально возможных угроз и каналов утечки информации;
    - Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
    - Определение требований к системе защиты.

РЕШЕНИЕ

- Выработка решения и подготовка ТЗ
  - Цель:
    - Разработка «Политики информационной безопасности».
  - Задачи
    - Осуществить выбор средств, методов, способов защиты информации и их характеристик;
    - Формализовать требования к средствам, методам, способам защиты информации с учетом многоуровневой модели ИТ;
    - Разработать техническое задание на проектирование системы обеспечения ИБ.

РЕШЕНИЕ

- Запроектировать выработанные решения
  - Цель
    - Получить проект реализации политики информационной безопасности, с учетом текущих проектов в смежных областях ИТ, на основании технического задания.
  - Задачи
    - Эскизное проектирование СОИБ;
    - Техническое проектирование СОИБ;
    - Рабочее проектирование СОИБ (включая документацию на используемые средства защиты, план ввода СОИБ в эксплуатацию и организационно-распорядительных документов по обеспечению информационной безопасности), планирование обучения пользователей и обслуживающего персонала.

РЕШЕНИЕ

- Реализация выработанного решения
  - Цель:
    - Обеспечение информационной безопасности ПАО «Татнефть».
  - Задачи:
    - Поставка программных и технических средств защиты информации;
    - Внедрение СОИБ;
    - Ввод СОИБ в эксплуатацию, настройка всех компонентов и подсистем, проведение приемо-сдаточных испытаний;
    - Обучение пользователей и обслуживающего персонала;
    - Аттестация объекта информатизации по требованиям безопасности информации в системе сертификации ФСТЭК (в случае необходимости);

РЕШЕНИЕ

- Сопровождение СОИБ
  - Цель:
    - Поддержание информационной безопасности
  - Задачи:
    - Мониторинг СОИБ;
    - Обслуживание СОИБ;
    - Поддержание работоспособности СОИБ;
    - Выявление новых угроз и реализация мер по их нейтрализации.