Киберпреступность в глобальных информационных сетях

Противодействие кибертерроризму

Взгляд оператора связи

Руководитель Департамента информационной безопасности Золотников А.Г.

6 октября 2008 г.

Объект исследования

- Глобальная информационно-телекоммуникационная сеть Интернет.
- Другие информационно-телекоммуникационные сети, где информация, информационные ресурсы, информационная техника могут выступать предметом преступных посягательств.

Цели использования сети Интернет террористическими группами (I)

- Сбор с помощью Интернета подробной информации о предполагаемых целях, их местонахождении и характеристике.
- Сбор денег для поддержки террористических движений.
- Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени встречи людей, заинтересованных в поддержке террористов, указаний о формах протеста и т.п., т.е. синергетическое воздействие на деятельность групп, поддерживающих террористов.
- Вымогательство денег у финансовых институтов, с тем чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.
- Вымогательство денег у финансовых институтов, с тем чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.
- Использование Интернета для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами с помощью Интернета широкой гласности своей ответственности за совершение террористических актов.

Цели использования сети Интернет террористическими группами (II)

- Использование Интернета для информационно-психологического воздействия, в том числе инициация «психологического терроризма». С помощью Интернета можно посеять панику, ввести в заблуждение, привести к разрушению чего-либо. Всемирная сеть — благодатная почва для распространения различных слухов, в том числе и тревожных, и эти возможности сети также используются террористическими организациями.
- Перенесение баз подготовки террористических операций. Поскольку электронам, в отличие от людей, «не надо предъявлять паспорт», терроризм больше не ограничен территорией того государства, где скрываются террористы. Более того, базы подготовки террористических операций уже, как правило, не располагаются в тех странах, где находятся цели террористов.
- Вовлечение в террористическую деятельность ничего не подозревающих соучастников — например, хакеров, которым не известно, к какой конечной цели приведут их действия. Кроме того, если раньше сеть террористов обычно представляла собой разветвленную структуру с сильным центром, то теперь это сети, где не просматривается четкая иерархия — такую возможность предоставляет Интернет.

Цели использования сети Интернет террористическими группами (III)

- Использование возможностей электронной почты или электронных досок объявлений для отправки зашифрованных сообщений.
- Размещение в Интернете сайтов террористической направленности, содержащих информацию о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также инструкции по их самостоятельному изготовлению.
- Атаки на информационные и компьютерные системы с целью противодействия их функционированию.
- Размещение на сайтах детской порнографии, информации, разжигающей национальную, расовую, религиозную вражду и т.д.
- Организация и проведение мошеннических операций на сетях связи с целью получения незаконных денежных средств для использования их в террористических целях.
- Атаки на телекоммуникационные сети операторов связи с целью нарушения их функционирования.

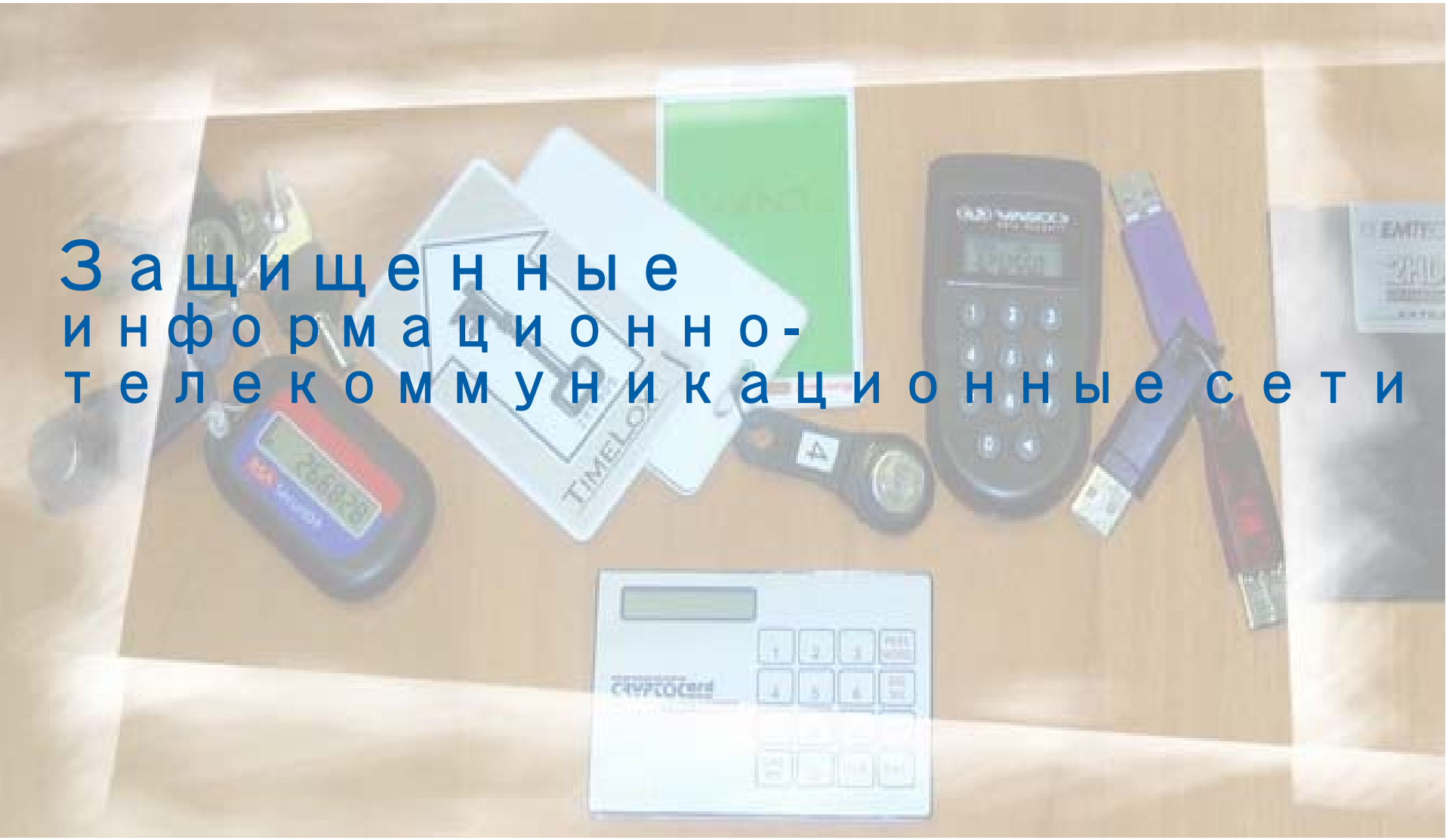
Роль оператора связи

Задачи оператора связи

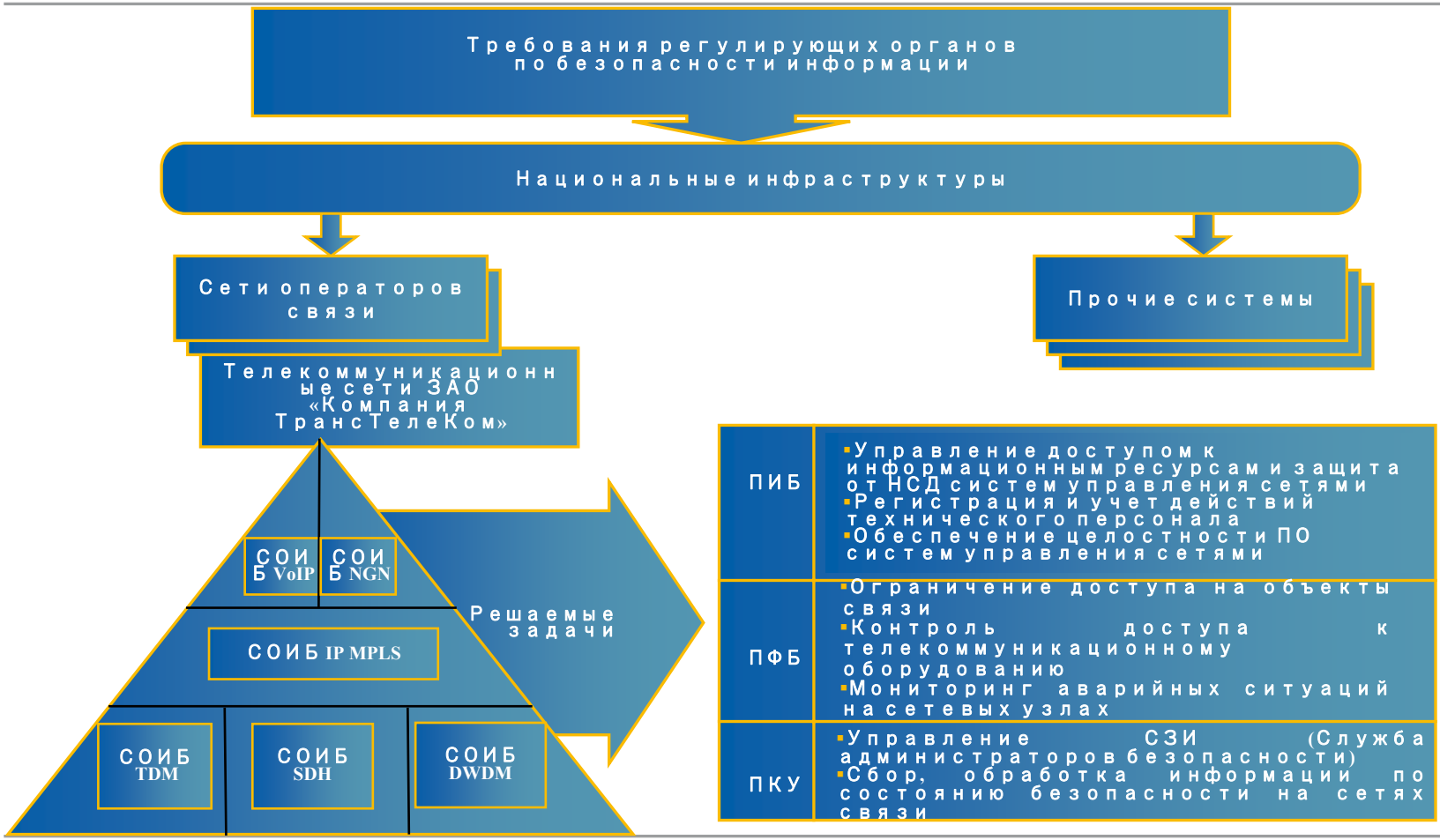
- Создавать защищенные информационно-телекоммуникационные сети.
- Разрабатывать и предоставлять клиентам защищенные информационно-телекоммуникационные услуги.
- Внедрять системы мониторинга информационно-телекоммуникиционных сетей.
- Внедрять системы противодействия мошенничеству.
- Осуществлять взаимодействие с правоохранительными органами и специальными службами.
- Осуществлять взаимодействие с другими операторами связи.
- Принимать участие в работе международных и национальных организаций.

КОМПАНИЯ ТТК

Защищенные информационно-телекоммуникационные сети



Многоуровневая система обеспечения информационной безопасности телекоммуникационных сетей ЗАО «Компания ТрансТелеКом»



Принципы создания защищённых ИТКС (ЗИТКС)

- Система управления – трёхуровневая: центр, регион, объект.
- Определение типовых системных структур ИТКС.
- Проведение работ по разработке и внедрению систем обеспечения информационной безопасности типовых системных структур ИТКС – создание защищённых ИТКС (ЗИТКС).
- Сертификация ЗИТКС по требованиям национальных нормативных документов, международных стандартов.
- Неизбыточность элементов СОИБ ИТКС.
- Проведение постоянного инструментального контроля достаточности мер защиты и доведение их до требований в случае отклонения (наличия новых требований).
- Информированность руководства о состоянии защиты ИТКС.
- Создание на базе ЗИТКС информационно-телекоммуникационных сетей клиентов и их аттестация.

КОМПАНИЯ ТТК

Создание и сертификация защищенных сетей

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 1166/1

Выдан 2 июня 2008 г.
Действителен до 2 июня 2011 г.

Настоящий сертификат удостоверяет, что **магистральная IP сеть ЗАО «Компания ТрансТелеКом»** (единичный экземпляр, маркированный знаком соответствия № А 376994), является автоматизированной системой общего назначения со встроенными средствами защиты, соответствует требованиям руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992) - по классу защищенности 1Г при условии выполнения требований технических условий ТУ АС-001-45922381-08.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЛИНС-М» (аттестат аккредитации от 07.10.2004 № СЗИ RU.907.Б027.060) - техническое заключение от 06.02.2006, экспертного заключения ФСТЭК России от 12.04.2006 и результатов инспекционного контроля, проведенного испытательной лабораторией ООО «ЛИНС-М» – заключение от 26.05.2008.

Заявитель: ЗАО «Компания ТрансТелеКом»
Адрес: 127006, г. Москва, ул. Долгоруковская, 7
Телефон: (495) 784-6685

Инспекционный контроль соответствия сертифицированной продукции требованиям указанных в настоящем сертификате руководящего документа и технических условий осуществляется испытательной лабораторией ООО «ЛИНС-М».

НАЧАЛЬНИК УПРАВЛЕНИЯ ФСТЭК РОССИИ

В. Селин

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 2 июня 2008 г.

- Создание защищенных телекоммуникационных сетей в соответствии с требованиями руководящих документов и их сертификация.
- Использование, при создании сетей связи и информационных систем, аппаратного и программного обеспечения, сертифицированного по требованиям информационной безопасности.

Создание и сертификация СМИБ

SGS

Certificate HU08/3058

The management system of

TransTeleCom Ltd.

7, Dolgorukovskaya str., Moscow, 127006, Russia

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2005

For the following activities

Control system of the IP-backbone

Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 27001:2005 requirements may be obtained by consulting the organisation

This certificate is valid from 13 February 2008 until 12 February 2011
Issue 1. Date of issue 13 February 2008
Certified since 13 February 2008

This is a multi-site certification
Additional site details are listed on the subsequent page

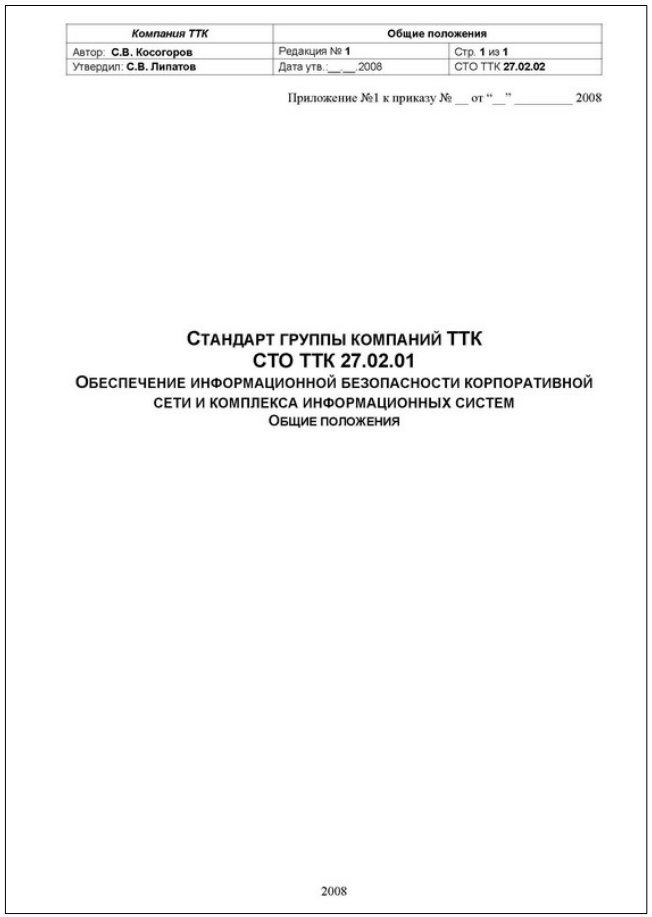
Authorised by

SGS United Kingdom Ltd Systems & Services Certification
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

Page 1 of 2

- Разработка и внедрение системы менеджмента информационной безопасности организации.
- Добровольная сертификация на соответствие ISO/IEC 27001:2005.
- Внутренний и сертификационный аудиты на соответствие требованиям стандарта.

Разработка корпоративных стандартов по ИБ



Компания ТТК	Общие положения	
Автор: **С.В. Косогоров**	Редакция № **1**	Стр. **1** из **1**
Утвердил: **С.В. Липатов**	Дата утв. __.__.2008	СТО ТТК **27.02.02**

Приложение №1 к приказу № __ от "__" _____ 2008

Стандарт группы компаний ТТК
СТО ТТК 27.02.01
Обеспечение информационной безопасности корпоративной сети и комплекса информационных систем
Общие положения

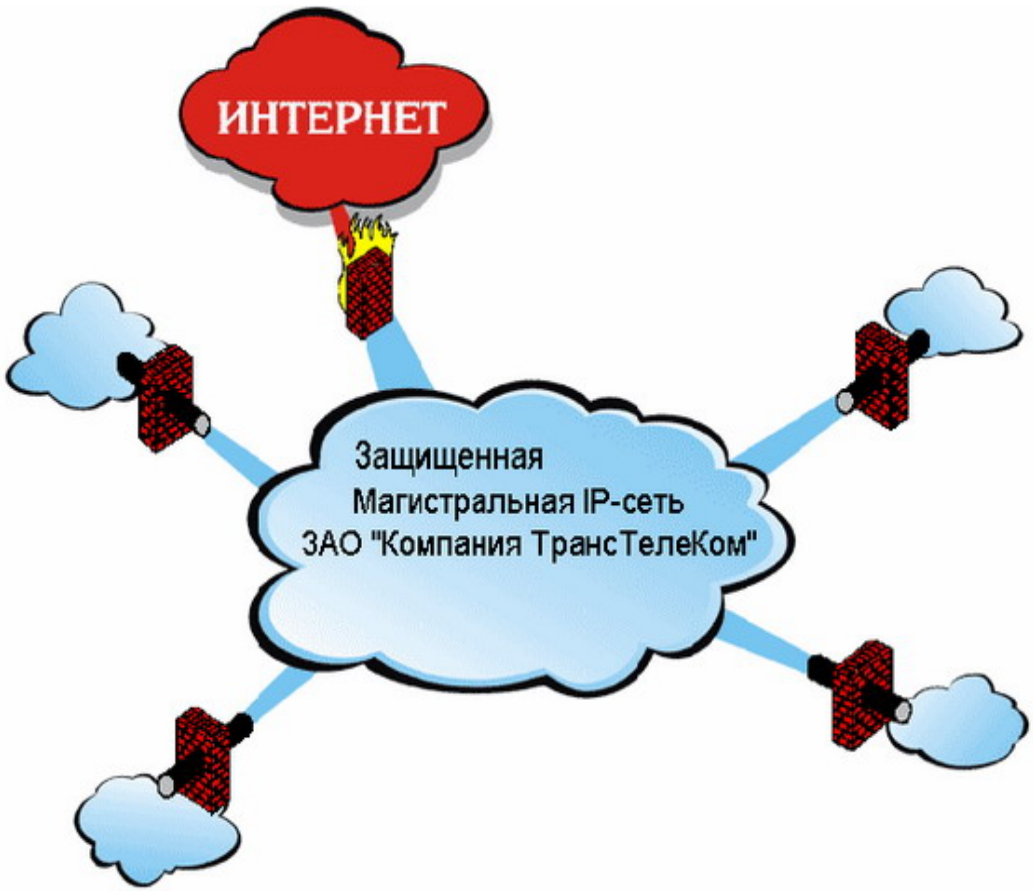
2008

- Унификация решений и требований по информационной безопасности в рамках корпорации.
- Разработка и внедрение стандартов организации по информационной безопасности.
- Внутренний аудит предприятий и подразделений на соответствие требованиям стандартов.

Защищенные информационно-телекоммуникационные услуги

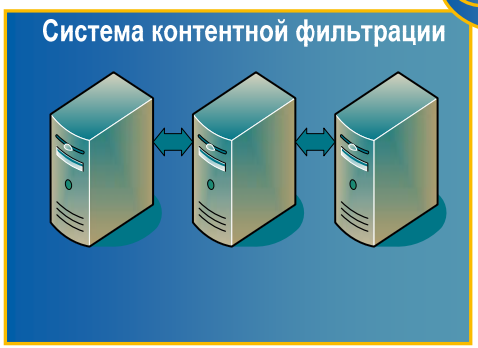
Защищенная информационная среда

Услуги информационной безопасности



- Доступ в Интернет из Виртуальной частной сети (ВЧС/IP VPN) Заказчика.
- Удаленный доступ к Виртуальной частной сети (ВЧС/IP VPN) Заказчика.
- Обеспечение криптографической защиты информации с использованием СКЗИ.

Контентная фильтрация информационных ресурсов

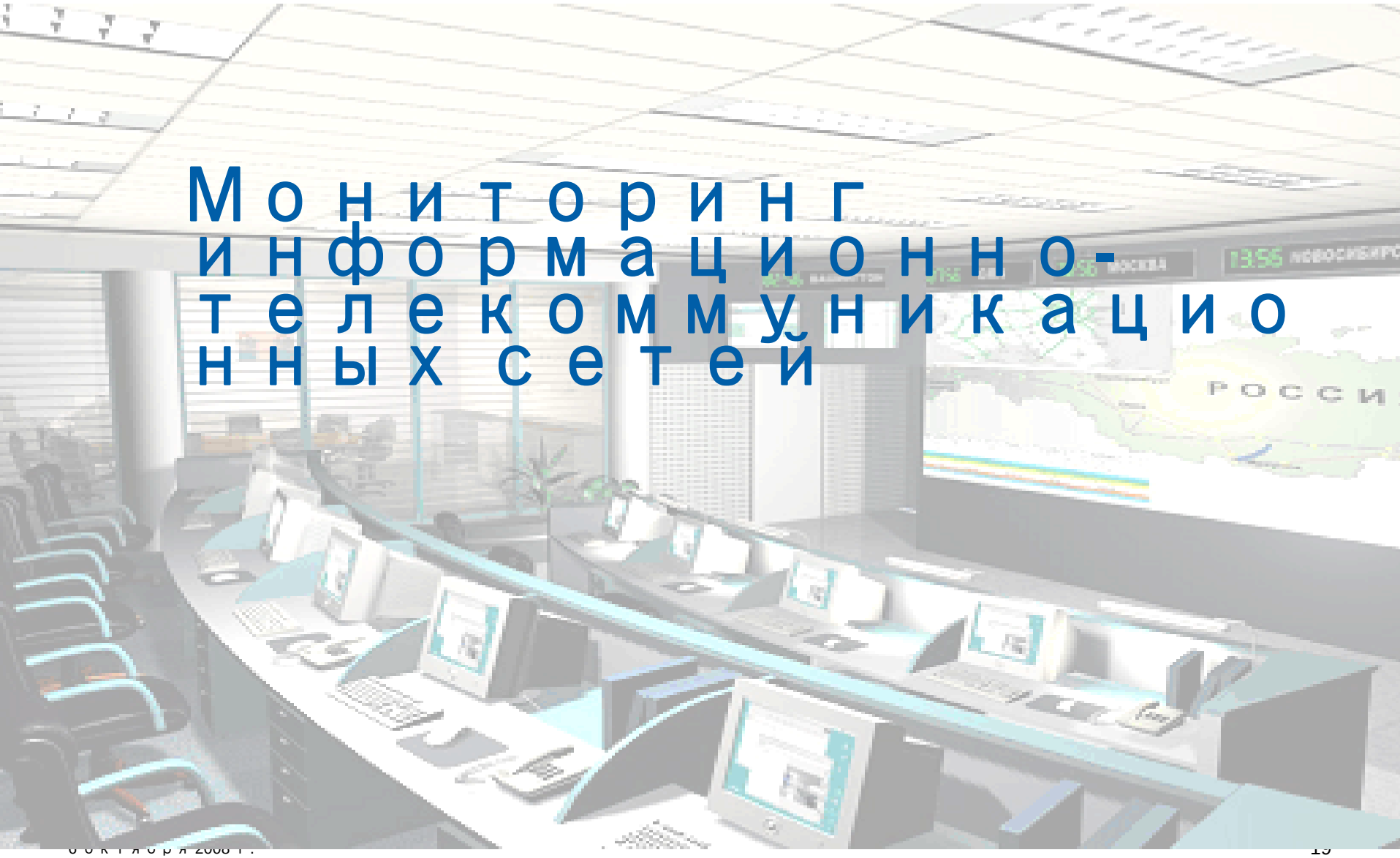


Функции контентной фильтрации

- исключение доступа пользователей к вредному и незаконному контенту, размещенному в Интернет;
- предотвращение утечки конфиденциальной информации при использовании Интернет (бесплатные почтовые сервисы, сайты, чаты, форумы и т.д.). Доля данного канала утечки составляет до 20%;
- исключение нецелевого расходования рабочего времени сотрудников имеющих доступ к Интернет;
- противодействие фишингу (рассылка писем от имени популярных компаний со ссылкой на сайт-двойник, на котором ничего не подозревающий пользователь сам оставляет свои идентификационные данные);
- борьба с фармингом (автоматическое перенаправление пользователей на фальшивые сайты, реализуемое с помощью специальных троянских программ, использующих уязвимости браузеров, операционных систем и DNS-серверов).

КОМПАНИЯ ТТК

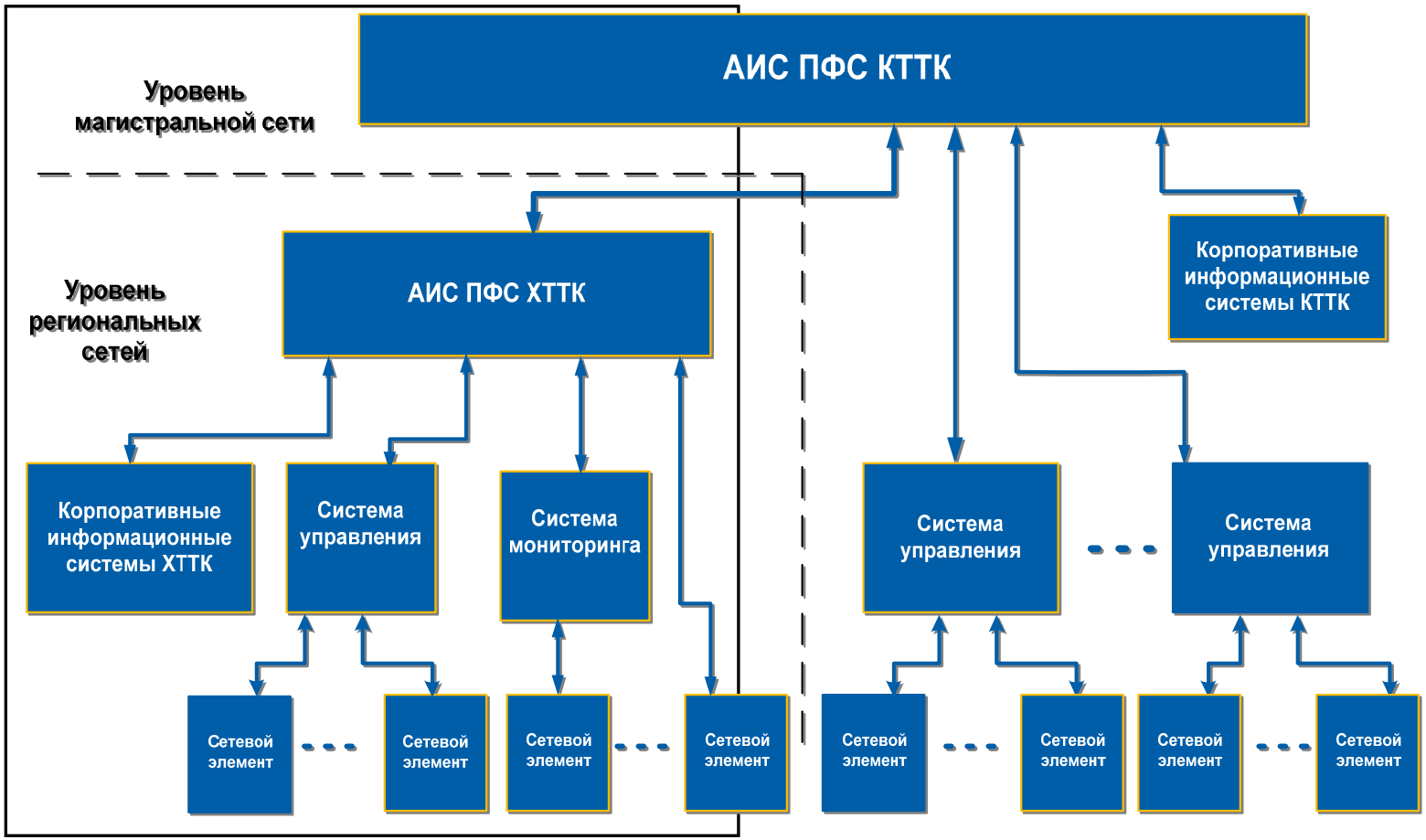
Мониторинг информационно-телекоммуникационных сетей



Задачи АИС ПФС

- Оперативный мониторинг параметров качества услуг и сетевых сервисов.
- Повышение эффективности использования сетевых ресурсов и улучшение качества планирования их развития.
- Повышение оперативности выявления сбоев в работе сетевого оборудования и его восстановления.
- Автоматизация сбора и обработки статистических данных по функционированию сетей.
- Повышение качества и оперативности обслуживания клиентов за счет четкой координации и информационной поддержки эксплуатационно-технических работ.
- Автоматизация процессов формирования и согласования планов проведения различных видов эксплуатационно-технических работ.
- Сокращение сроков проведения эксплуатационно-технических работ.
- Автоматизация учета сетевых ресурсов и контроля за их использованием.

Структура АИС ПФС группы Компаний ТрансТелеКом



Внедрение систем мониторинга трафика

- Федеральный Закон РФ №. 126-ФЗ от 07.07.2003 г. «О связи», Статья 64.
- Федеральный Закон РФ №. 40 от 03.04.1995 г. «Об органах Федеральной службы безопасности в РФ».
- Указ Президента РФ №. 891 от 01.09.1995 г.
- Приказ Министерства связи РФ №. 226 от 24.06.1992 г.
- Приказ Госкомсвязи РФ №. 47 от 27.03.1999 г.
- Приказ Минсвязи РФ №. 130 от 25.07.2000 г.
- Постановление Правительства №..538 от 27 августа 2005 г.
- Требования телекоммуникационных лицензий.

Противодействие DOS-атакам

Целью DOS атаки является блокирование нормального функционирования отдельного информационного ресурса или всей сети оператора связи.

Система противодействия DOS атакам состоит из:

- подсистемы обнаружения DOS атаки;
- подсистемы фильтрации DOS атаки.

Наличие системы противодействия DOS позволяет оператору связи в режиме реального времени предотвращать доступ «паразитного» трафика в сеть потребителя услуги.

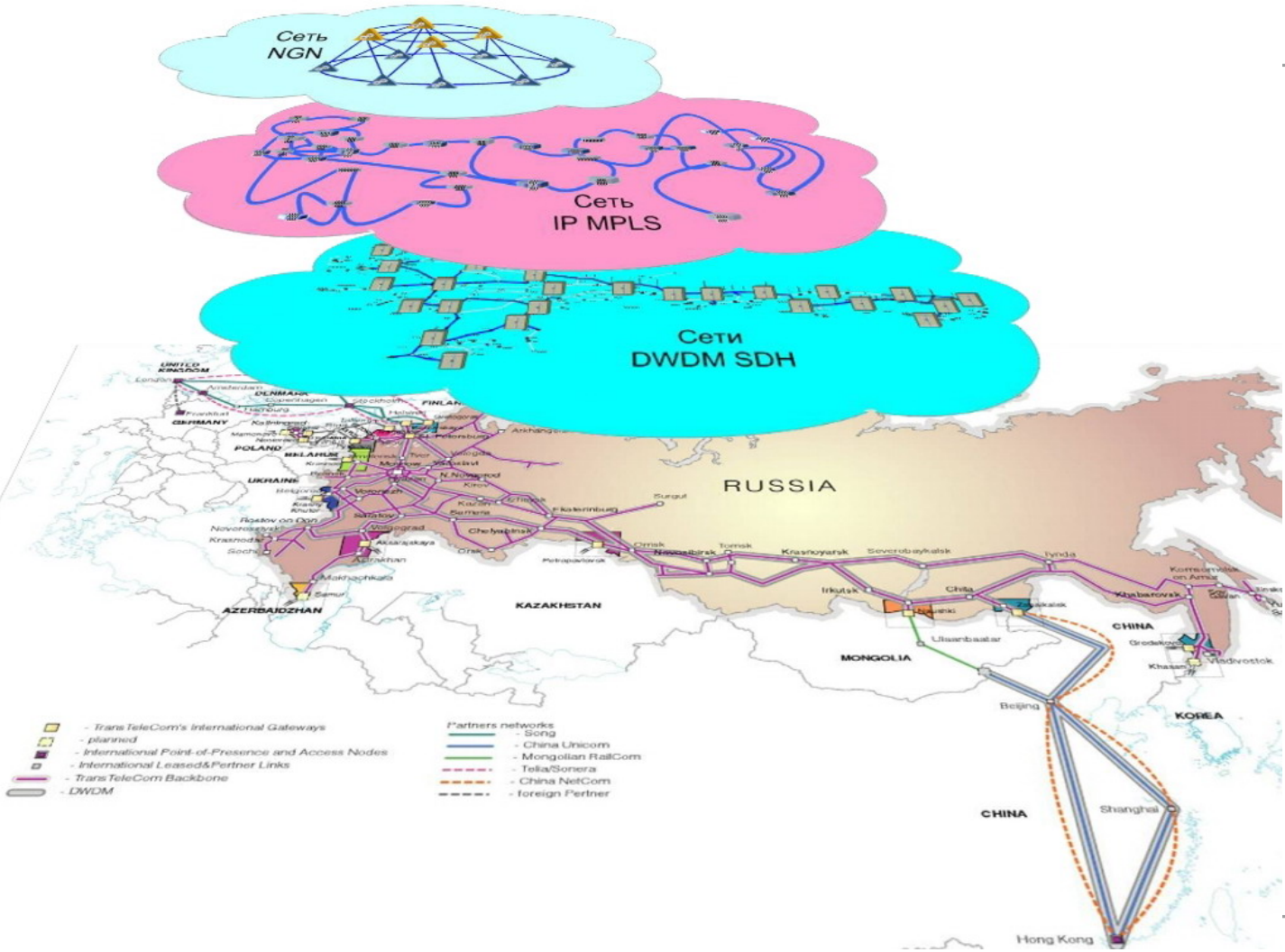
КОМПАНИЯ ТТК

Системы противодействия мошенничеству

Актуально – неактуально?

- Потери от мошенничества составляют десятки миллиардов долларов. 2005 год: $55-60 млрд. – 5% совокупного дохода всех телекоммуникационных операторов (CFCA).
- Ежегодный рост потерь от мошенничества – 10-15% (CFCA).
- В н.в. по оценкам экспертов насчитывается порядка 200 видов мошенничества. Число их постоянно растет.
- Все крупные и большинство средних зарубежных операторов имеют системы FMS.
- Имидж оператора.

Сеть связи современного оператора



Каталог продуктов

- **Аренда каналов**
  - NPL
  - IPL
  - ЦКС
  - Канал доступа
- **Голосовые услуги**
  - Местная связь
  - Дальняя связь (оферта)
  - Дальняя связь(письменный договор)
  - Услуги при соединения и пропу трафика
  - Услуги 800
  - Услуги ЦОВ
  - IP Centrex
  - FMC
  - Персональный номер
  - Виртуальный офис
  - Интернет-телефония
  - Voice VPN
  - Prepaid calling cards
- **Передача данных**
  - IP VPN
  - IP VPN Port-Port
  - IP VPN SLA
  - Корпоративная сеть связи
  - GPRS IP VPN
  - Доступ к ФТС
  - Комплексная корпоративная сеть связи
  - Ethernet Private Line
  - IP Multicast
  - Доступ к финансово-Информационным ресурсам
  - Услуги MEN
- **Доступ в Интернет/телематика**
  - Доступ в Интернет
  - Data Transit
  - Комплексный доступ в Интернет
  - Услуги присоединения и пропуска трафика
  - Internet security
  - Internet managed access
  - Видеоконференц-связь
  - Видео-телефония
- **IP TV**
  - IP TV
  - Video-on-demand
  - Personal Video Recorder
- **Data Center**
  - Disaster recovery
  - Colocation
  - Hosting services
- **Дополнительные услуги**
  - Монтаж и подключение оборудования
  - Синхронизация сетей связи
  - Информационный портал
  - ЭЦП
  - CPE Service
  - MVNO
  - Unified Messaging
  - Системная интеграция
  - Call Center

Мошенничество на SDH сети

Услуги	Угрозы мошенничества	Краткое описание
Аренда каналов связи	**Несанкционированное использование каналов связи**	**Передача не предусмотренного договором трафика**
	Регистрация по подложным документам	**Фальсификация данных в контракте с целью уклонения от оплаты**
	Неоплата услуги в период тестирования	**Внутреннее мошенничество**
	Неотключение услуги после закрытия контракта	**Внутреннее мошенничество**
	Несанкционированное предоставление услуги	**Внутреннее мошенничество**

Мошенничество на IP сети

Услуги	Угрозы мошенничества	Краткое описание
Передача данных, телематика (VPN, доступ в Интернет)	Регистрация по подложным документам	Фальсификация данных в контракте с целью уклонения от оплаты
	Неполный учет трафика	Некорректная обработка (генерация) данных для тарификации
	Неправильное применение тарифов	Стоимость услуги может быть различна для коммерческих и государственных структур
	Искажение тарифов	Неправомерное изменение тарифа
	Неправильное техническое обслуживание телекоммуникационного оборудования (изменение конфигураций)	Конфигурация оборудования не в соответствии с подписанным контрактом (увеличение полосы пропускания, доп. услуги и др.)
	Нарушение доступности услуги	DDoS-атаки
	Нарушение информационной безопасности сети	НСД к оборудованию сети

Мошенничество на NGN-сети

Услуги	Угрозы	Краткое описание
Голосовые услуги, дополнительные услуги	Маскирование международного трафика под местный	На сеть оператора приземляют трафик и исходящий международный номер прописывается как местный
	Предоставление PRS-услуг	Генерация ложных вызовов владельцев PRS- сервисов
	Переадресации вызовов	Подмена номера при переадресации вызовов.
	Нарушение доступности услуги	Атаки типа «отказ в обслуживании» (DoS)
	Взлом АТС	Нарушение нормального функционирования АТС с целью организации нелегальных звонков через данную АТС
	Распространение, модификация внутренней информации	Внутреннее мошенничество: пополнение счетов и нелегальное добавление услуг, передача конф. информации третьим лицам

Мошенничество на NGN-сети (продолжение)

Услуги	Угрозы	Краткое описание
Голосовые услуги, дополнительные услуги	Использование алгоритмов маршрутизации	Звонок в страны А из страны В дешевле, чем наоборот, поэтому в стране В установлено устройство для автоматического повторного набора номера, через который осуществляется вызов нужному абоненту по более низкому тарифу
	Звонки на направления HRC – High Risk Countries (Египет, Вьетнам, Китай и др.)	При нелегитимных подключениях оператор подвержен риску неоплаты МН соединений, либо конфликтных ситуаций с оплатой таких соединений и потерей лояльности абонентов, оборудование которых было незаконно использовано
	Рефайлинг/Тунелирование	Передача трафика через VoIP
	Сговор операторов для пропуска трафика при различных тарифных планах	Актуально при различных ценах на одно направление для разных присоединенных операторов
	Пропуск сигнального и голосового трафика по разным направлениям	Пропуск сигнального трафика через оператора, а голосового через альтернативные маршруты (VoIP)

Последствия мошенничества

- Длительные или кратковременные потери доходов и рост расходов оператора.
- Рост давления на операторов связи с целью снижения тарифов.
- Ухудшение качества сети, что приводит к росту инвестиций для поддержания уровня необходимого сервиса.
- Отказы от оплаты по счетам.
- Проблемы во взаиморасчетах с другими операторами связи.
- Неудовлетворенность уровнем услуг и жалобы со стороны абонентов, их отток.
- Снижение репутации оператора.

Противодействие мошенничеству

- Организационные меры (организация отдельной службы по борьбе с мошенничеством в составе аналитиков и технического персонала).
- Процедурные меры (разработка процедур, регламентов).
- Технические меры (внедрение аппаратно-программных средств противодействия мошенничеству, внедрение системы обеспечения информационной безопасности).

КОМПАНИЯ ТТК

Взаимодействие с правоохранительными органами и специальными службами

Предоставление правоохранительным органам и спецслужбам для оперативного обмена информацией:

- Высоконадежных каналов связи (Кг = 0,9999).
- Каналов с необходимой пропускной способностью (в н.в. емкость сети КТТК составляет до 40 Гбит/с).
- Защищенных, в соответствии с требованиями регулирующих органов, сетей и каналов связи, позволяющих осуществлять передачу конфиденциальной информации.

Создание условий и осуществление деятельности в области противодействия несанкционированному доступу к информационным ресурсам в соответствии с требованиями регулирующих органов, что подтверждается соответствующими лицензиями.

Организация и проведение обучения сотрудников правоохранительных органов и специальных служб по вопросам обеспечения информационной безопасности на телекоммуникационных сетях и защиты информационных ресурсов в рамках создания современных высокопроизводительных защищенных телекоммуникационных систем.

- Обмен опытом в рамках проведения круглых столов, семинаров и конференций по проблемам противодействия киберпреступности.
- Участие сотрудников Компании в работе коллегий научно-технических советов, рабочих совещаниях и комиссиях по проблемам противодействия киберпреступности.

- Взаимодействие дежурных служб и структурных подразделений Компании, правоохранительных органов и спецслужб для оперативного пресечения киберпреступлений (фрод-атаки, несанкционированное вмешательство, взлом серверов и рабочих станций, хищение конфиденциальной информации).
- Участие в работе совместных комиссий по расследованию случаев киберпреступлений.

Взаимодействие с операторами

- Заключение двухсторонних и многосторонних соглашений (договоров) по организации совместных действий.
- Участие в национальных и международных организациях.
- Проведение рабочих встреч и обмен опытом.
- Участие в конференциях и семинарах.

Работа в международных и национальных организациях

- АДЭ (Ассоциация Документальной Электросвязи)
- ЕВРААС (Евро-Азиатская Ассоциация производителей товаров и услуг в области безопасности)
- CFCA (Communications Fraud Control Association)
- FIINA (Forum for International Irregular Network Access)

Контакты

ЗАО «Компания ТрансТелеКом»
127006, Москва, ул. Долгоруковская, д.7
Тел: +7 (495) 784 66 70
Факс: +7 (495) 784 66 71
www.transtk.ru
Info@transtk.ru