



КОМПАНИЯ ИТК

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



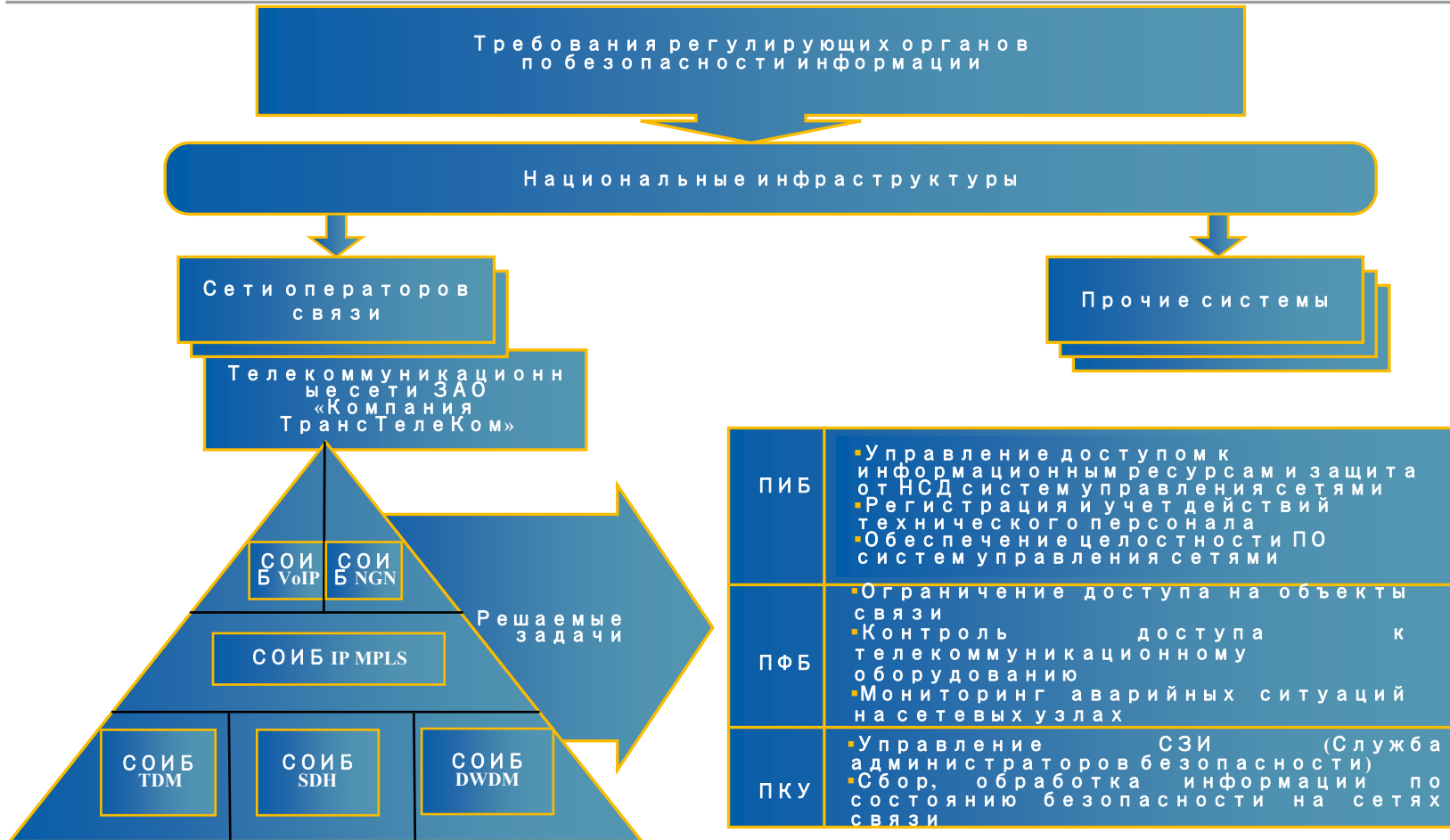
# Задачи оператора связи



- Создавать защищенные информационно-телекоммуникационные сети.
- Разрабатывать и предоставлять клиентам защищенные информационно-телекоммуникационные услуги.
- Внедрять системы мониторинга информационно-телекоммуникационных 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.

# 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.

# Создание и сертификация защищенных сетей

- 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.

**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 ИГ 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 и сертификация СМИБ



- 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

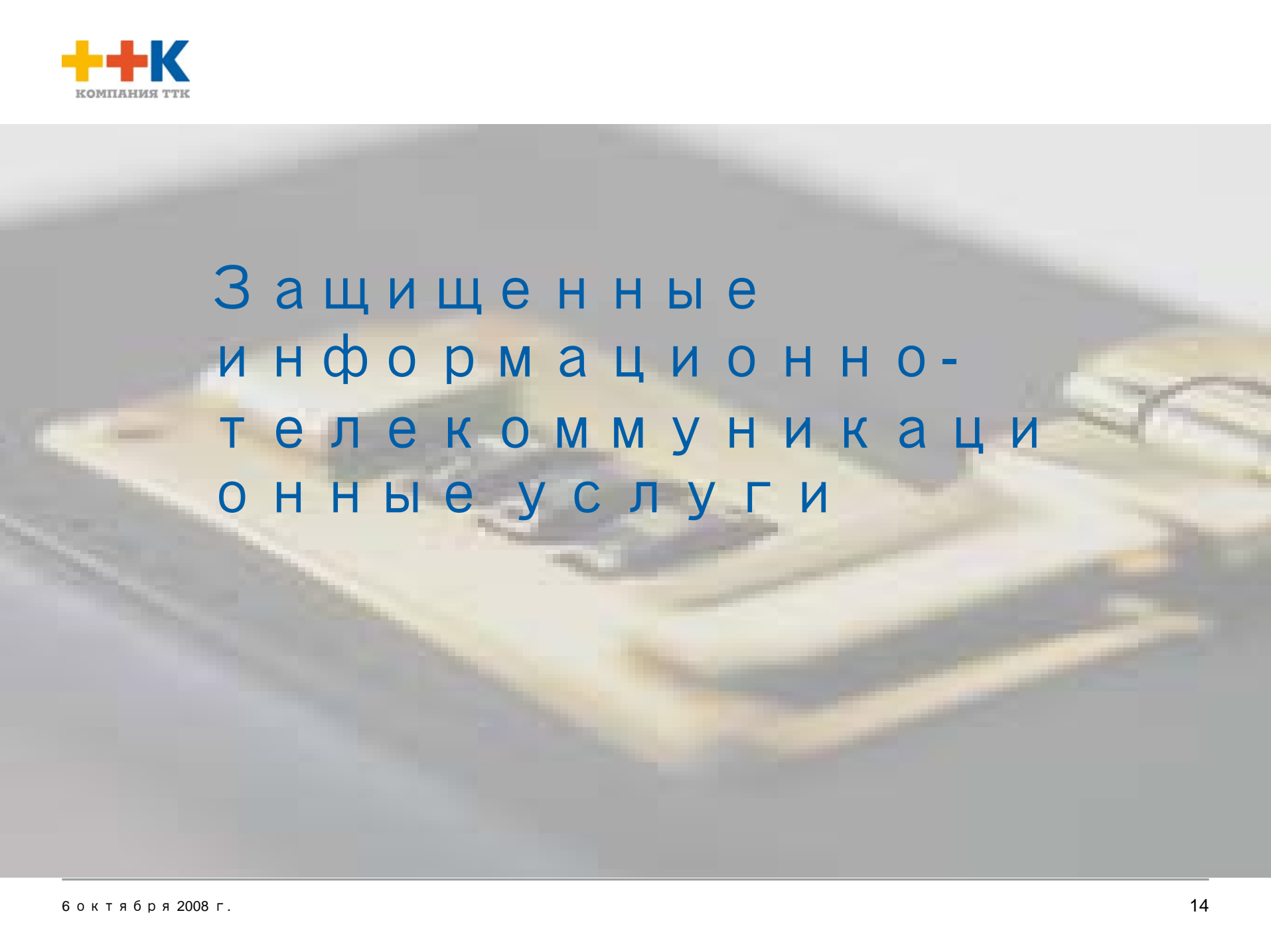
Компания ТТК		Общие положения	
Автор: С.В. Косогоров	Редакция № 1	Стр. 1 из 1	
Утвердил: С.В. Липатов	Дата утв. ____ 2008	СТО ТТК 27.02.02	

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.



З а щ и щ е н н ы е  
и н ф о р м а ц и о н н о -  
т е л е к о м м у н и к а ц и  
о н н ы е у с л у г и

# Защищенная информационная среда



# Услуги информационной безопасности

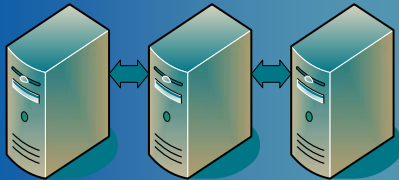


- Доступ в Интернет из Виртуальной частной сети (ВЧС/IP VPN) Заказчика.
- Удаленный доступ к Виртуальной частной сети (ВЧС/IP VPN) Заказчика.
- Обеспечение криптографической защиты информации с использованием СКЗИ.

# Контентная фильтрация информационных ресурсов



Система контентной фильтрации



# Функции контентной фильтрации



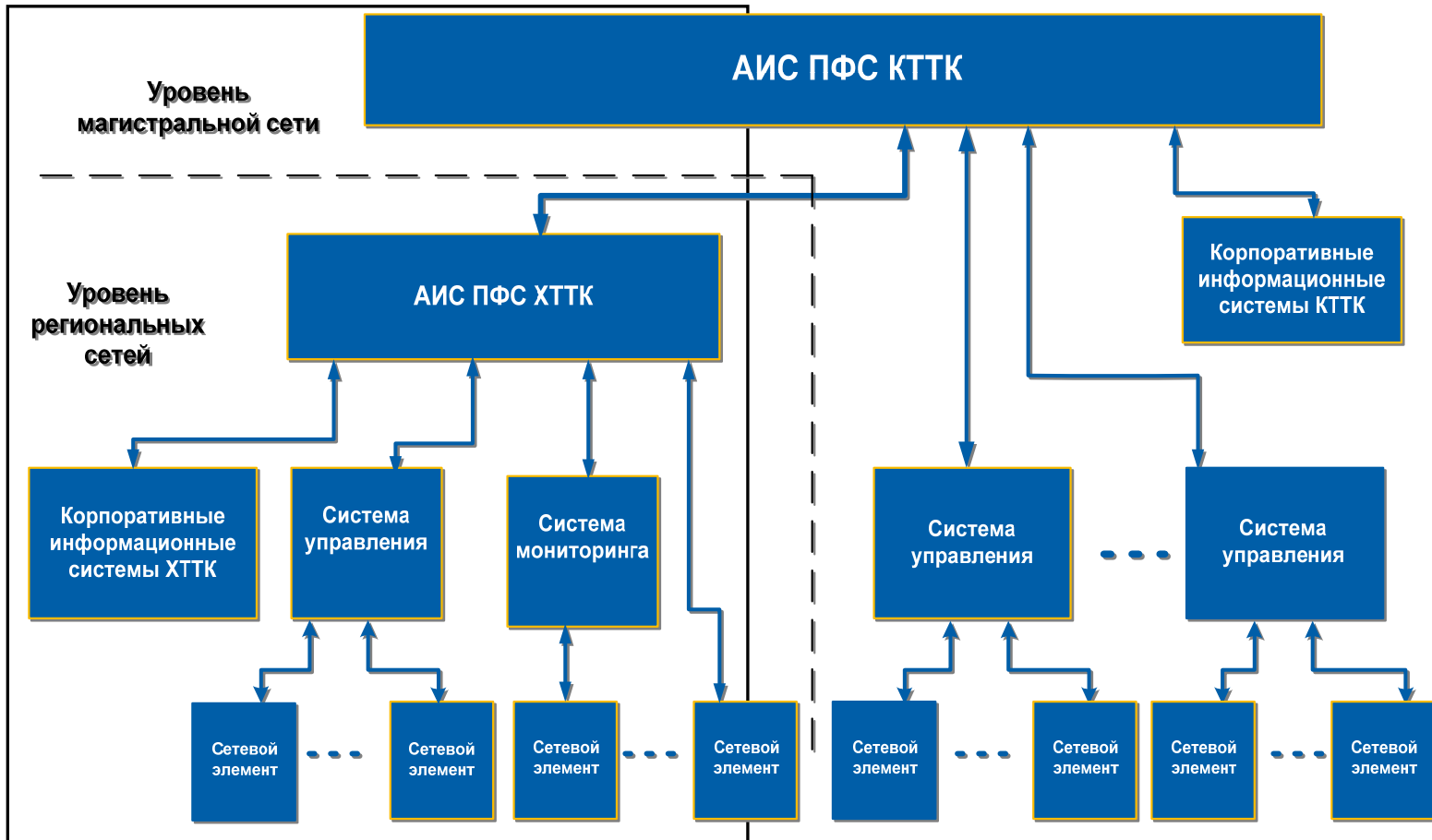
- исключение доступа пользователей к вредному и незаконному контенту, размещенному в Интернет;
- предотвращение утечки конфиденциальной информации при использовании Интернет (бесплатные почтовые сервисы, сайты, чаты, форумы и т.д.). Доля данного канала утечки составляет до 20%;
- исключение нецелевого 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).

# Мониторинг информационно- телекоммуникацио- нных 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 атак 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.

---

С и с т е м ы  
п р о т и в о д е й с т в и  
я м о ш е н н и ч е с т в у



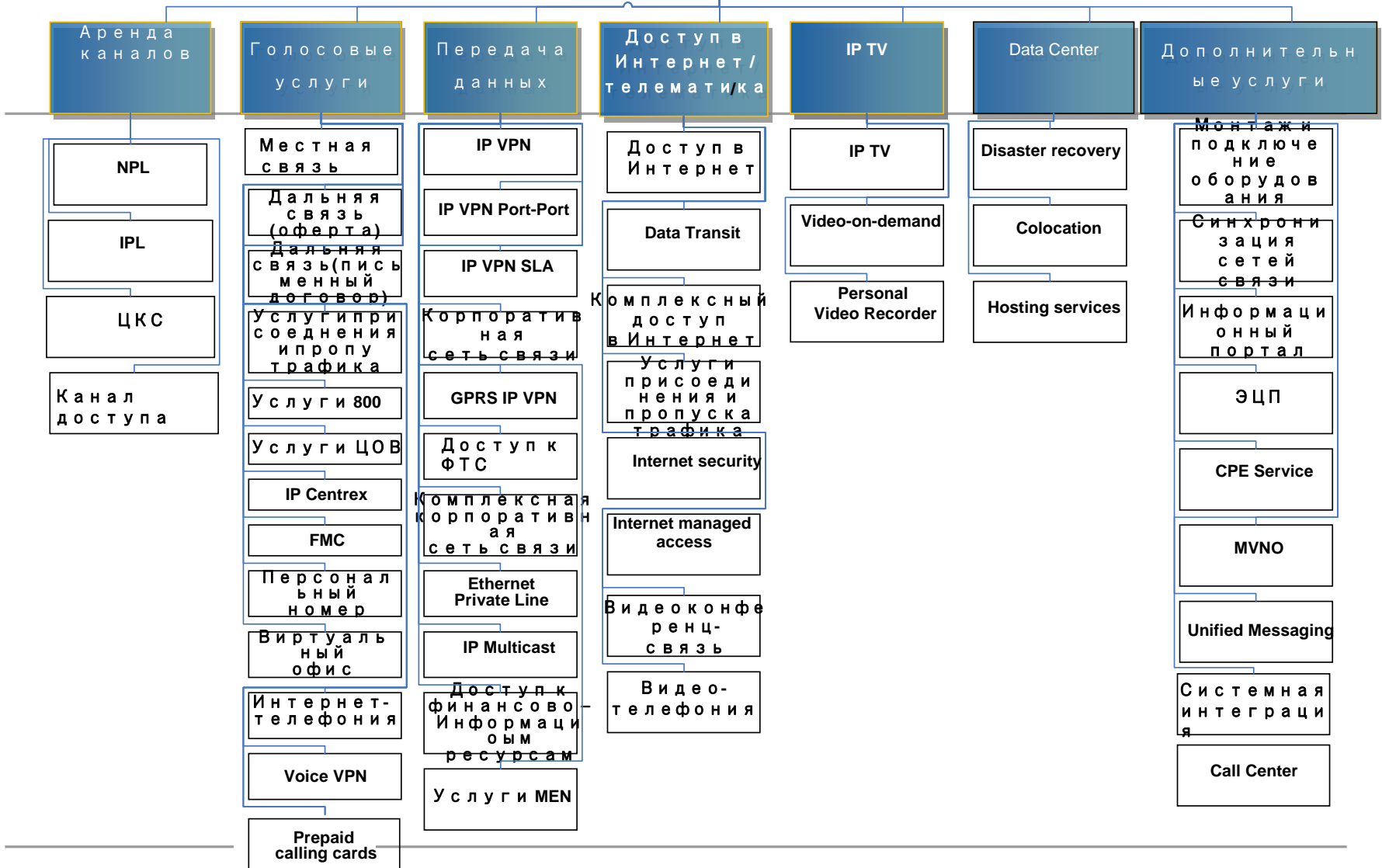
# А к т у а л ь н о – н е а к т у а л ь н о ?

---

- 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 растёт.
- Все крупные и большинство средних зарубежных операторов имеют системы FMS.
- Имидж оператора.



# Каталог продуктов



# Мошенничество на SDH сети

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

# Мошенничество на IP сети

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

# Мошенничество на NGN-сети (продолжение)

Услуги	Угрозы	Краткое описание
<b>Голосовые услуги, дополнительные услуги</b>	<b>Использование алгоритмов маршрутизации</b>	<b>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</b>
	<b>Звонки на направления HRC – High Risk Countries (Египет, Вьетнам, Китай и др.)</b>	<b>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</b>
	<b>Рефайлинг/Тунелирование</b>	<b>Передача трафика через VoIP</b>
	<b>Сговор операторов для пропуска трафика при различных тарифных планах</b>	<b>Актуально при различных ценах на одно направление для разных присоединенных операторов</b>
	<b>Пропуск сигнального и голосового трафика по разным направлениям</b>	<b>Пропуск сигнального трафика через оператора, а голосового через альтернативные маршруты (VoIP)</b>

# П о с л е д с т в и я м о ш е н н и ч е с т в а

- 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).

В з а и м о д е й с т в и е с  
п р а в о о х р а н и т е л ь н ы м и  
о р г а н а м и и  
с п е ц и а л ь н ы м и  
с л у ж б а м и

# Предоставление правоохранительным органами и спецслужбам для оперативного обмена информацией:

---

- Высоконадежных каналов связи ( $K_{г} = 0,9999$ ).
- 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.

---

С о з д а н и е у с л о в и й и  
о с у щ е с т в л е н и е  
д е я т е л ь н о с т и в о б л а с т и  
п р о т и в о д е й с т в и я  
н е с а н к ц и о н и р о в а н н о м у  
д о с т у п у к и н ф о р м а ц и о н н ы м  
р е с у р с а м в с о о т в е т с т в и и с  
т р е б о в а н и я м и  
р е г у л и р у ю щ и х о р г а н о в , ч т о  
п о д т в е р ж д а е т с я  
с о о т в е т с т в у ю щ и м и  
л и ц е н з и я м и .



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)

# К о н т а к т ы

---

З А О «К о м п а н и я  
Т р а н с Т е л е К о м»  
127006, М о с к в а, у л.

Д о л г о р у к о в с к а я, д.7

Т е л: +7 (495) 784 66 70

Ф а к с: +7 (495) 784 66 71

[www.transtk.ru](http://www.transtk.ru)

[Info@transtk.ru](mailto:Info@transtk.ru)