МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ

«МЕХАНИЗМЫ БЕЗОПАСНОСТИ В СЕТЯХ ПОСТ NGN, 4G, 5G, ИСПОЛЬЗУЕМЫХ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЯМИ ПРОИЗВОДСТВА»

ДОКЛАДЧИК: профессор кафедры Информационной и кибернетической безопасности Учебно-научного института защиты информации к.т.н., доцент ГУЛАК Г.Н.

План доклада

1. Типовые уязвимости системы обеспечения кибербезопасности.
2. Факторы, обуславливающие рост проблем в обеспечении кибербезопасности
3. Угрозы безопасности в сети пост NGN (транспорт АСУ ТП) и механизмы защиты.
4. Модель злоумышленника.
5. Модель угроз и риски криптоанализа.
6. Защита от угроз имитации.
7. Анализ вариантов реализации СКЗИ.
8. Схема построения СКЗИ.
9. Оценка безопасности СКЗИ.
10. Выводы.

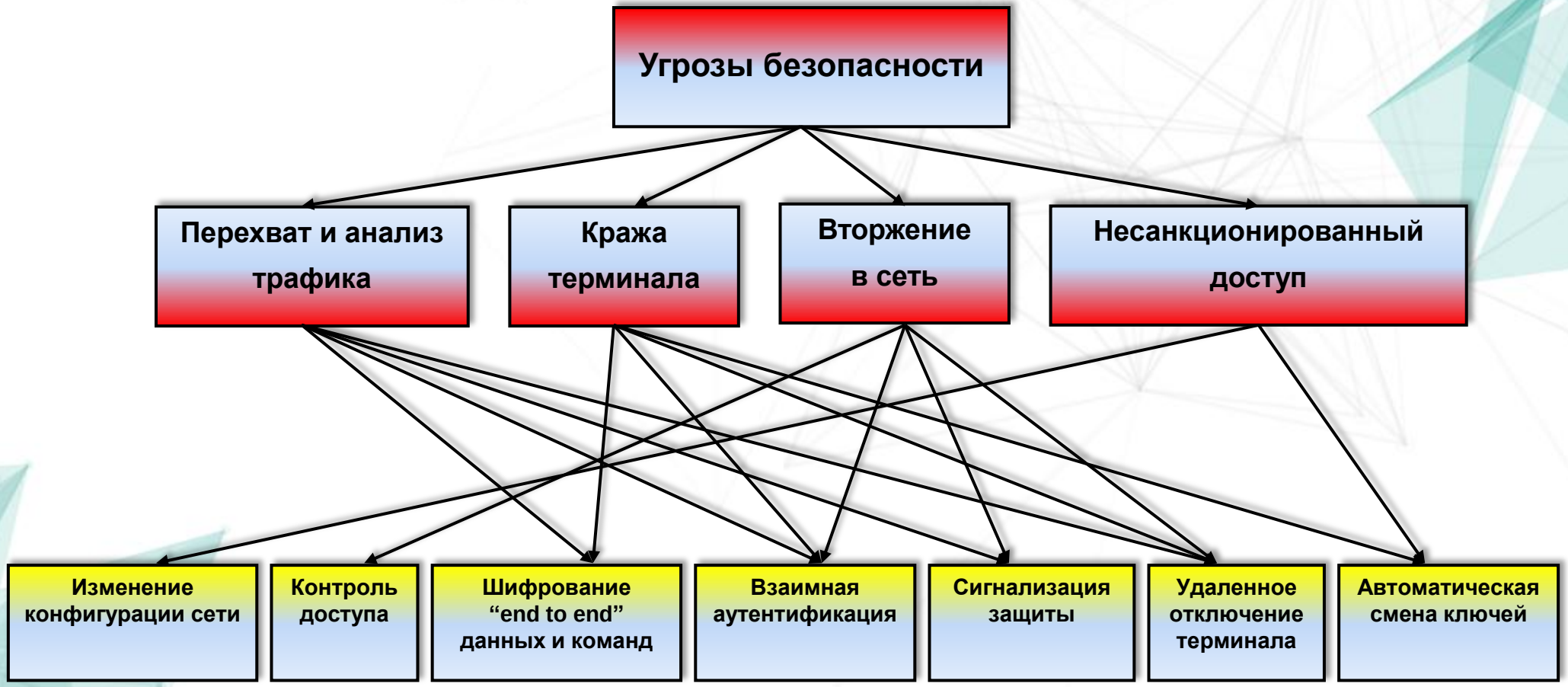
Типовые уязвимости системы обеспечения кибербезопасности

- ***несоответствие*** уровня развития инфраструктуры электронных коммуникаций современным требованиям к ее безопасности, особенно в высокотехнологичных отраслях (энергетика, транспорт, химические производства и т.д.);
- ***недостаточный уровень*** защищенности от киберугроз информационной инфраструктуры, электронных информационных ресурсов и информации, требования по защите которой установлена законом;
- ***бессистемность мер*** киберзащиты критической информационной инфраструктуры;
- ***недостаточное развитие*** организационно-технической инфраструктуры обеспечения кибербезопасности и киберзащиты критической информационной инфраструктуры и электронных информационных ресурсов;
- **недостаточная эффективность** противодействия киберугрозам военного, криминального, террористического характера;
- ***недостаточный*** уровень координации, взаимодействия и информационного обмена между общественностью и субъектами обеспечения кибербезопасности.

Факторы, обуславливающие рост проблем в обеспечении кибербезопасности

- Быстрое развитие сетевых технологий, включая внедрение сетей пост NGN, 4G. 5G, опережает развитие регуляторных механизмов, нормативных требований к системам и средствам защиты.
- Атаки становятся все более сложными, регулярными и совершенными.
- Выявление атак происходит уже после их завершения, если такое вообще происходит.
- Атаки реализуются с помощью вредоносных кодов и технологий анонимизации, что позволяет злоумышленникам преодолевать определенные защитные барьеры.
- Системы наблюдения за проникновением, базы данных антивирусов быстро устаревают и не обеспечивают необходимого уровня безопасности.
- Злоумышленники успевают использовать уязвимости инноваций раньше, чем разработчики систем их устраняют или создают необходимые инструменты.

Угрозы безопасности в сети пост NGN (транспорт АСУ ТП) и механизмы защиты



Модель злоумышленника

Относительно злоумышленника допустимы следующие предположения.

Злоумышленник:

- знает алгоритм шифрования, но не знает действующего ключа;
- имеет доступ к транспортной сети;
- может считывать в сети любые сообщения;
- может заменять передаваемое сообщение на любое другое или формировать и вставлять в канал любое сообщение;
- может выполнять все действия без существенной задержки.

.

Модель угроз и риски криптоанализа

- **КА только по Тш**

(Ciphertext only attack)

- **КА с известным То**

(Known plaintext attack)

- **КА с выбранным То**

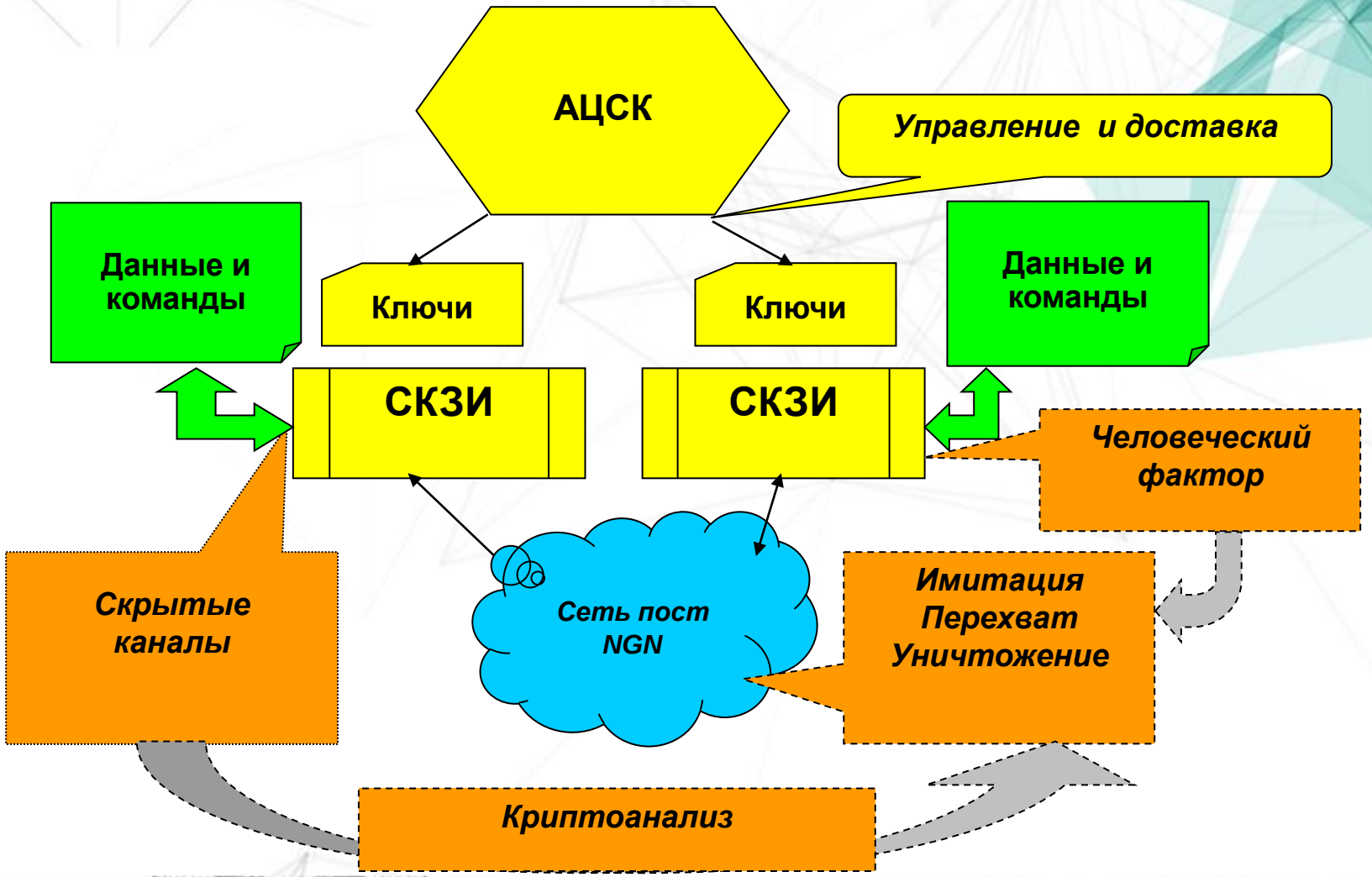
(Chosen plaintext attack)

- **КА с выбранным Тш**

(Chosen ciphertext attack)

•Атаки по побочным или скрытым каналам используют критическую информацию, перехваченную от СКЗИ (не Тш или То).

•Примеры атак АСК: с помощью регистрации ПЭМИН, данных энергопотребления, вибро-акустических волн, ошибок вычислений, обработки ошибок в канале связи, измерения времени выполнения, доступа до кэш-памяти и т.д.



Защита от угроз имитации

Имитостойкость (*imitation resistance*) – свойство криптосистемы, характеризующее ее способность противостоять активным атакам со стороны злоумышленника, целью которого является навязывание ложного сообщения, подмена передаваемого сообщения или изменение данных. Ложная информация считается навязанной, если она принята приемным устройством к исполнению.

Основные способы имитозащиты:

- Смена ключей по «плавающему» графику.
- Использование отметок времени.
- Внесение избыточности в текст, например, с помощью кодирования.
- Использование имитовставок (*message authentication code - MAC).*
- **Применение имитостойкого шифрования** с помощью псевдослучайной последовательности подстановок замены: $X_1, X_2, \dots, X_m, \dots$.

Анализ вариантов реализации СКЗИ

Варианты реализации СКЗИ:

- **Программное средство (ПС)** представляет собой исполняемый код в среде типовой ОС компьютера со стандартной комплектацией**:**
- **Программно-аппаратное средство (ПАС)** отличается от предыдущего варианта реализацией основных криптографических примитивов микроэлектронными устройствами;
- **Аппаратное средство (АпС)** предполагает полную реализацию всей криптосхемы на основе микроэлектронных схем в виде самостоятельного устройства**.**

Тип реализации	Преимущества	Недостатки
ПС	1. Невысокая стоимость изделия. 2. Гибкость по отношению к технологиям транспортного уровня	1. Слабая защищенность от атак на реализацию 2. Невысокая производительность.
ПАС	1. Повышенный уровень безопасности 2. Повышенная производительность	1. Средний уровень защиты от атак на реализацию 2. Повышенная стоимость
АпС	1. Высокая производительность 2. Известные механизмы блокировки побочных каналов утечки	1. Самая высокая стоимость 2. Ориентация на конкретные протоколы

Схема построения СКЗИ

Вхід синхронізації

Вхід синхронізації

Ключ *K*

Ключ *K*

Вектор *IV*

Вектор *IV*

Генератор ПСП шифратора А (ДСТУ 7624:2014)

Генератор ПСП шифратора Б (ДСТУ 7624:2014)

Система контроля и блокировки

To

Алгоритм генерации *Xm*

Транспортная сеть

Алгоритм генерации *Xm*

To

Оценка безопасности СКЗИ

$$Q = \frac{\max \Pi_{\text{т}}}{\min\{C_{AA}, C_{AP}, C_{AK}\}}$$

Где: Пт – ущерб от атак

C_{AA} - цена атаки на алгоритм шифрования;

C_{AP} - цена атаки на реализацию средства защиты (инженерно-криптографическая);

C_{AK}– цена атаки по побочным каналам утечки информации (ПЭВМН);

Q – относительная оценка эффективности защиты.

Варианты:

Q<<1 – высокий уровень безопасности;

Q =1 – средний уровень безопасности;

Q>1 – низкий уровень безопасности.

Выводы

1. Для обеспечения требуемого уровня имитостойкости разработан алгоритм генерации подстановок замены на основе псевдослучайной последовательности, полученной с помощью алгоритма блочного шифрования (ДСТУ ГОСТ 28147:2009, ДСТУ 7624-2014) в режиме OFB.

2. Алгоритм генерации обеспечивает необходимые вероятностные характеристики и имеет быстродействие в среднем в 4 раза превышающее производительность метода бесповторного набора подстановок замены.

3. Предложенный алгоритм колонной (многоалфавитной) замены допускает 8 кратное повторение ключа без снижения стойкости шифрования.

4. Сложность подмены сообщения длины L оценивается величиной 15^L

5. На основе статистической задачи о разладке предложен критерий выявления атак на программную реализацию СКЗИ, что обеспечивает необходимую оперативность реакции при практических применениях.

Спасибо за внимание!