# Некоторые тенденции в изменении ландшафта угроз информационной безопасности и средств безопасности

*Курило Андрей Петрович*
*Председатель Комитета*
*по информационной безопасности НП НСФР*

# Особенности методологического подхода к защите информации

- Работая в сфере безопасности  мы имеем дело с вероятностными процессами и судить о них можно только в терминологии рисков. В том числе, и оценивать уровень безопасности.
- Оценить безопасность информации нельзя. Можно только оценить качество свойств безопасности среды, в которой живет информация или системы защиты этой среды.

# Внешние факторы

Усиление напряжения во внешнеполитической сфере

**Санкции**.

*Реакция*:

- Импортозамещение;
- Постепенный уход большого числа иностранных вендеров:
  - Лицензионные риски
  - Возникающее отставание в применении современных технологий

Заказчики начинают требовать российские продукты

В течение нескольких лет проблем не создает

**Усиление хакерской активности в политических целях:**

- Рост числа DDoS – атак
- Изменение целей атак

*Реакция:*

- Активизация по созданию системы «Сопка»
- Корректировка моделей угроз
- Повышение уровня «готовности» СОИБ и IT инфраструктур к отражению атак

# Технические факторы: ландшафт угроз, новые возможности и технологии

- Ландшафт угроз изменяется крайне медленно, вместе с тем, актуальность некоторых угроз возростает, что несколько видоизменяет ландшафт
- Дальнейшая профессионализация преступных групп, занимающихся киберпреступлениями
- Появление нового класса высокотехнологических угроз  - APT это опасно!

# Изменения ландшафта инцидентов и направлений деятельности по повышению безопасности операций

Факторы влияния:

1. Возникающий дефицит денег:
   - Тонизирует рост преступных атак:
     - При этом, технических специалистов, способных организовать технологически сложные атаки больше не стало, а стараниями ПМВД России их становится несколько меньше. Новых быстро подготовить сложно.

*Последствия*:

- Перенос усилий на физические атаки (банкоматы, инкассаторы, обменные пункты, банки)
- Социальная инженерия
- Уход на мошенничество с документами (вопрос плохо изучен, но отголоски информации позволяют сделать вывод о том, что это очень криминализированная сфера)

2. Модификация м улучшение систем ЭСП:
   - Введение чиповых карт
   - отказ от использования магнитной полосы
   - Повышение защищенности банкоматов, терминалов
   - Введение элементов технологии 3D Secur
   - Ограничение по числу карт, телефонных счетов, переводимым суммам

Рост числа случаев скиминга остановился

3. Слабые места, *последствия*:
   - операции с электронными документами
     - Поворот в сторону технологии 3D Secur, единых хранилищ ЭД
   - Возникающие трудности поддержки технологии при массовом использовании УКЭП:
     - Поворот в сторону ПЭП
   - Неудовлетворительно решена задача проведения аутентификации
     - Поворот в сторону ЕСИА

# Новые угрозы

1. Атаки типа APT. Нацелены на кредитные организации, а не на клиентов. Ущерб растет, объемы разовых хищений растут.
2. Атаки, направленные в большей степени на отказ в обслуживании и нарушение непрерывности бизнеса, чем на хищения. В этом случае масштаб ущерба в целом для государственных институтов больше (пример- физическая атака на инфраструктуру энергоснабжения). Нацелены на IT -инфраструктуры государственных институтов.
3. Атаки на канал подтверждения:
   - Использование слабостей в технологии передачи данных
   - Подмена СИМ-карты

   Нацелены на физических лиц.
4. Атаки вирусов на приложения, размещенные на мобильных телефонах с целью подмены данных или подтверждений.

   Нацелены на физических лиц.

# Вопрос, старый как мир

Какой путь повышения защищенности выбрать:

- Повышения уровня защиты путем усложнения модели угроз
- Повышения качества работы системы безопасности

Что лучше: неуверенно работающая новая или хорошо работающая старая технология?

Почему на сработала система безопасности и  стали возможны последние теракты и катастрофы?

# Ближайшие инициативы

- Корректировка законодательства о связи с целью получения возможности создания информационной системы по переходящим номерам.
- Корректировка ФЗ О персональных данных с целью легализации работы по обмену данными по «Дропам»
- Распространение в практической деятельности ПЭП, особенно на финансовом рынке
- Совершенствование массового механизма аутентификации на базе ЕСИА

# Факторы влияния на рынок средств безопасности

- Рецессия
- Секвестирование бюджетов
- Импортозамещение
- Увеличение циклов обновления ПК

- Появление SOC как инструмента централизации управления безопасностью
- Централизация администрирования IT- инфраструктур
- Постепенная смена парка оборудования

# Спасибо за внимание

А.П. Курило,
НП НСФР