# Моделирование устойчивости систем к кибератакам

Наличие процессора или памяти в технической структуре представляет потенциальную опасность кибернападения внешнего или внутреннего нарушителя

# Оценка устойчивости начинается с модели компьютерной части системы

- АСУ ТП может иметь различные уровни влияния на ТП. Модель конечна-действительность бесконечна. Все оценки в рамках моделей
- Три уровня моделирования компьютерной системы(КС)

1. Описание физических сущностей, составляющих КС, и

транспортная модель физических, а поверх них логических связей

2. Модель уровня основных базовых продуктов (Биос, ОС, СУБД, Криптосистема, система хранения данных и т.д.)

3. Перечень прикладных задач и их взаимосвязей как между собой так и с уровнями 1.и 2.

Выделение подсистем, относящихся к или использующих 1,2,3. и подлежащих особому контролю (ПД, КИИ, конфиденциальная информация)

Формирование на основе модели уровней устойчивости всей системы: полная работоспособность, достаточная работоспособность, минимально необходимая, катастрофа

# Тестирование на проникновение и устойчивость-моделирование нападения

- Возможные цели тестирования со стороны владельца КС:
- а) поиск уязвимостей, приводящих к установленному уровню устойчивости;
- б) анализ системы на выявление узких мест выполнения функционала;
- в) анализ «естественной» устойчивости при непреднамеренных действиях персонала;
- г) импорто-зависимая часть, подлежащая замещению
- Согласование плана тестирования и фиксации достигнутых результатов:
- а) согласование применяемых методов (подбрасывание зараженных флешек?);
- б) пределы воздействия тестировщиков на отдельные элементы;
- в) фиксация и способы предъявления результатов тестирования

# Моделирование способов воздействия и добычи дополнительной информации

- Моделирование и методы реализация DDOS атаки- масштабы и объекта воздействия.
- Пределы Закона на нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ); незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ); неправомерный доступ к компьютерной информации (ст. 272 УК РФ).
- Фишинг- на кого в КС охота? Кого подвергаем тестированию?
- Социальная инженерия и глубина анализа данных. Только Интернет?
- При реализации тестирования и сбора информации нельзя переходить рамки закона
- Применение принципа «песочницы», ее место размещения и оценка адекватности исследуемой КС
- Модель ныне действующего хакера, внутреннего и внешнего нарушителя. В какой степени помогает модель нарушителя от ФСТЕК

# Оценка защищенности и надежности криптомеханизма в обеспечении устойчивости

- Устойчивость шифрсвязи(ШС) по каналам, выходящим за пределы КЗ. Последствия применения байпаса при разрушении ШС
- Использование возможности обхода криптозащиты через ППО. Что давать тестировщикам по составу ППО? Вариант: ничего или некоторую общеизвестную часть
- Моделирование признания не легитимной электронной подписи(ЭП)
- Моделирование использования с помощью ППО нештатной ЭП или не допущенного ключевого носителя
- Моделирование обхода биометрического барьера для нарушения принадлежности ЭП истинному владельцу

# Оценка киберустойчивости это моделирование будущего нападения

- Прогнозирование ценности информации и устойчивости КС-моделирование целей будущего нападения. Выбор временных периодов. Когда может быть нападение
- Прогнозирование развития методов нападения на ближайшее будущее это значит до следующего тестирования
- «Квантовые» системы вычислений будут представлять угрозу для парольных систем с хранимыми значениями хеш паролей? Подмена элементов ППО возможна для систем с контролем целостности на хеш функциях?
- Массовое применение слабых систем защиты информации пользователями может порождать принципиально новые методы нападения на локальные КС
- Как часто надо проводить тестирование КС на проникновение и устойчивость?

# Моделирование нападения на массового не корпоративного пользователя

- Модель «обычного» пользователя –гражданина с домашней компьютерной системой: Wi-Fi—провайдер, PC, смартфон, ТВ, пылесос, автомобиль и т.д.
- Что защищать? Удаленный банкинг, сессию с удаленным рабочим местом, личную переписку в электронной почте, тревогу от угона автомобиля и т.д.
- Массовый пользователь абсолютно технически слабо защищен и легко подвергается социальному инжинирингу, ключ ЭП на простой флешке, подписание документа в оперативной памяти PC
- DDOS –атака легко организуется по причине отсутствия навыков борьбы и экранов низкой эффективности и сложности настройки
- Вывод: моделировать нападение могут и уже частично реализуют под прикрытием массового пользователя или группы пользователей