КОНФЕРЕНЦИИ «БЕЛЫХ ХАКЕРОВ» И СПЕЦИАЛЬНЫЕ ИССЛЕДОВАТЕЛЬСКИЕ ИГРЫ КАК ЧАСТЬ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА.

Жукова Дарья
СПбГУ ИТМО БИТ

Хакерские конференции

Название	Проводится	Место проведения	Сайт
DefCon	1993 г., ежегодно	Лас- Вегас	www.defcon.org
LAYER ONE	2004 г., ежегодно	Лос-Анджелес	www.layerone.info
Toorcon	1998 г., ежегодно	Сан-Диего	www.toorcon.org
BlackHat	1997 г., ежегодно	Вашингтон	www.blackhat.com
CCC	1984 г., ежегодно	Берлин	www.ccc.de
What the Hack?	1989 года, каждые 4 года	Нидерланды	www.whatthehack.org
EUSecWest	С 2005 г., ежегодно	Лондон	http://eusecwest.com/
CanSecWest	С 2001 г., ежегодно	Ванкувер	http://cansecwest.com
Hack in the Box	С 2003 г., ежегодно	Малайзия, АОЭ, Дубай	www.hackinthebox.org
Power of Community	С 2006 г., ежегодно	Южная Корея	www.powerofcommunity.org
PacSec	С 2002 г., ежегодно	Токио	http://pacsec.jp/index.html

Становление хакерских съездов

Цели хакерских конференций

Тематика хакерских конференций

- Привлечение внимания к информационной безопасности;
- Сбор информации, обмен опытом борьбы с «кибертерроризмом»;
- Реализация предупреждающих стратегий;
- Демонстрация новейших решений в области управления информационной безопасностью;
- Разработка инструментов для защиты системы от возможных угроз;
- Обсуждение проблем социальных аспектов хакерства и др.

Защита

- Принципы построения системы безопасности объекта;
- Оценка эффективности и выработки предложений по модернизации системы безопасности;
- Выявление жизненно важных целей и предметов защиты предприятия, организации;
- Анализ уязвимостей, классификация возможных угроз. Разработка модели угроз и нарушителей;
- Управление ИБ.
- Защита от вредоносных программ

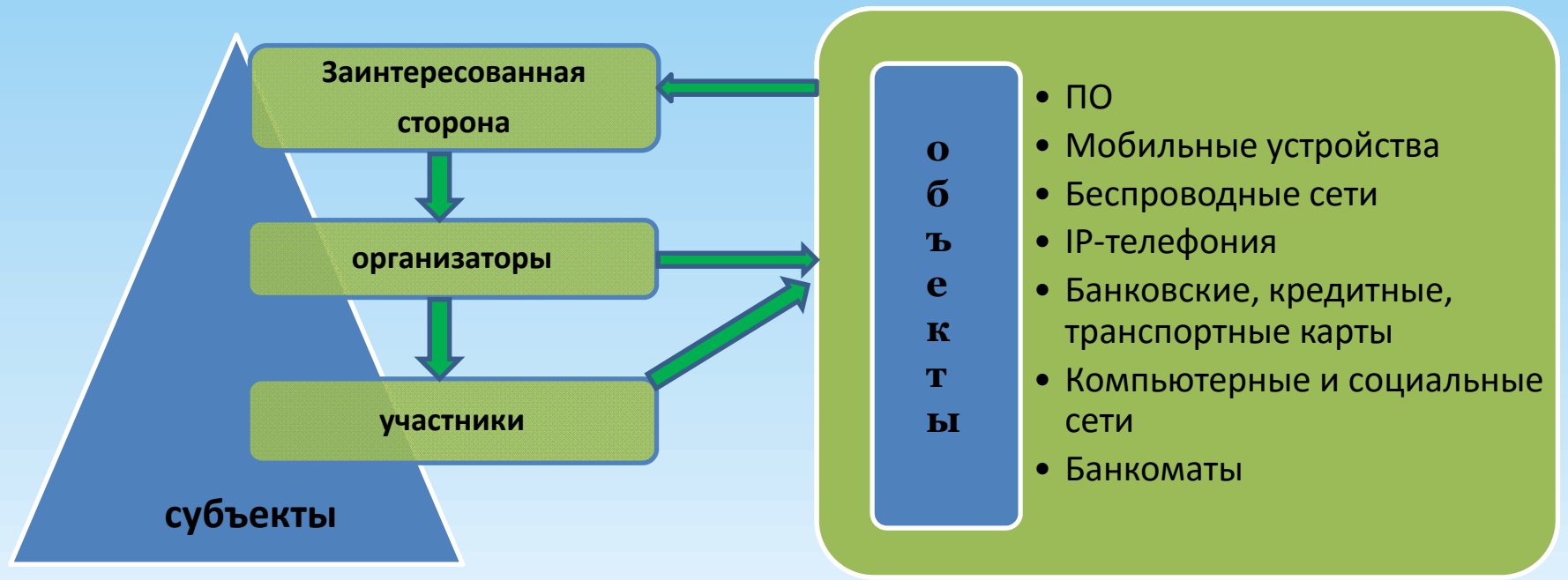
Нападение

Демонстрация технологий и методов

- Поиска и эксплуатации уязвимостей;
- Скрытого перехвата информации;
- Анонимного проведения атак;
- Реализации различных типов атак (DoS, MITM, Injection etc.);
- Атак на криптографические алгоритмы;

«Особенности» оборудования

Модель угроз ИБ в рамках конференции хакеров




Угрозы
Атаки на мобильные устройства
Использование НДВ
Восстановление данных с утилизованного носителя
Ботнеты
Изменение подлинности данных
Сторонние приложения
Подмена IP
Атаки на не-Windows системы
Виртуальные системы

Capture The Flag!

Название	Место проведения	Сайт
DefCon	Лас-Вегас	www.defcon.org
UCSB iCTF	University of California	ictf.cs.ucsb.edu/
CIPHER	Германия	www.cipher-ctf.org

Отборочный этап

Финальные сорвенования

Квесты

Сервисы

Квесты

Системное администрирование

Программирование

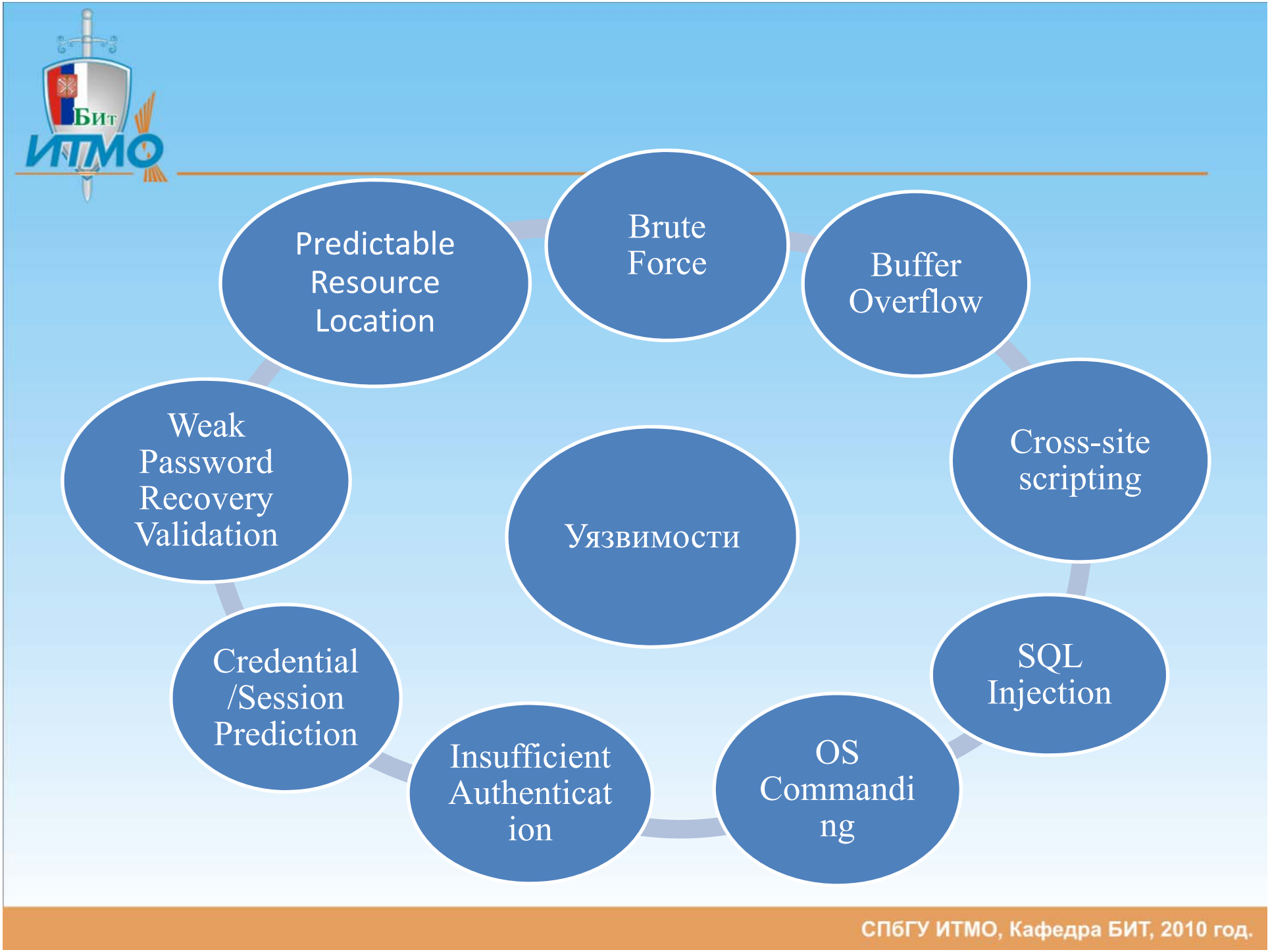
Криптоанализ

Стеганоанализ

Криминилистика

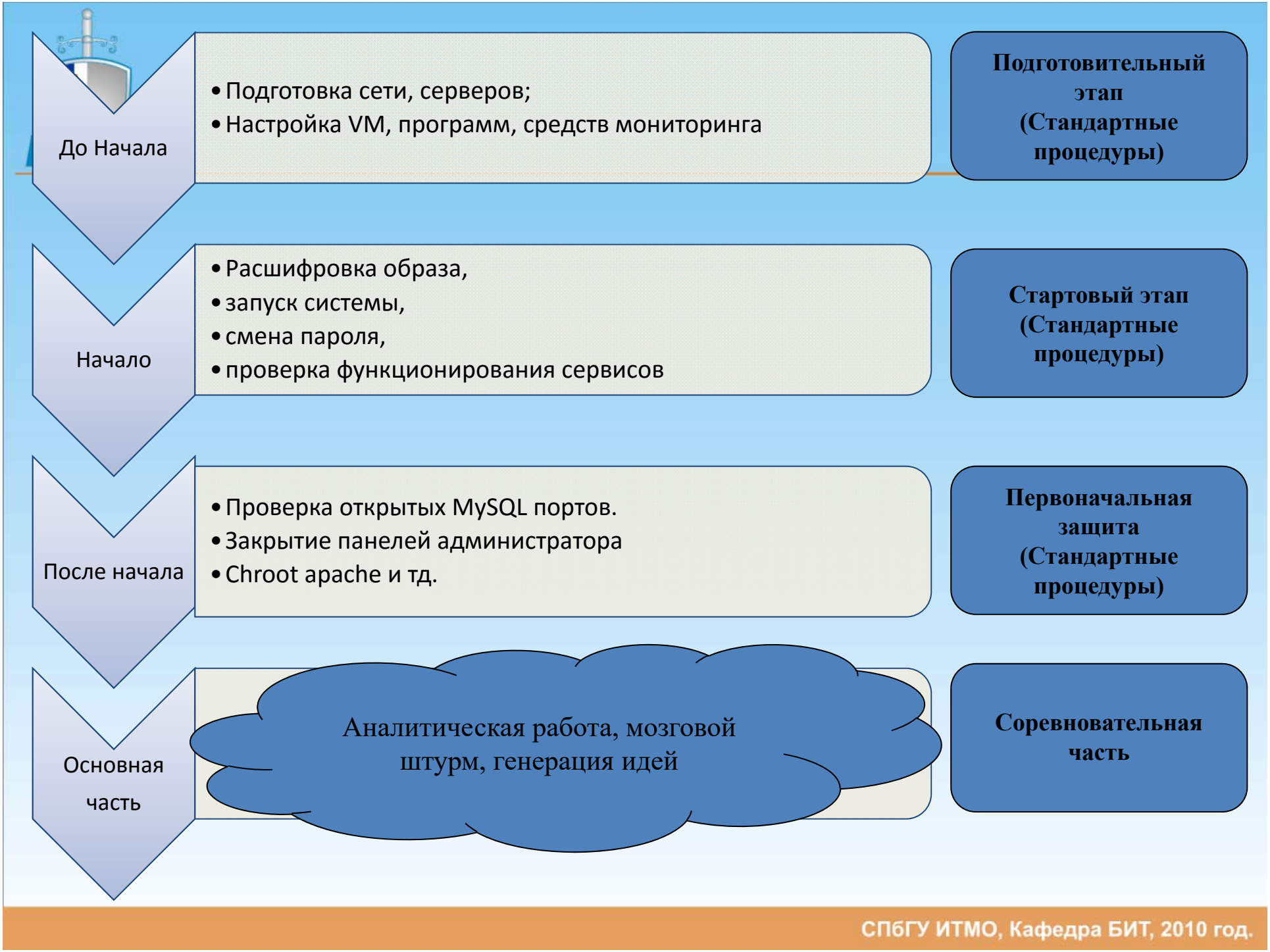
Reverse Engineering (анализ машинного кода программ)

GoogleFoo

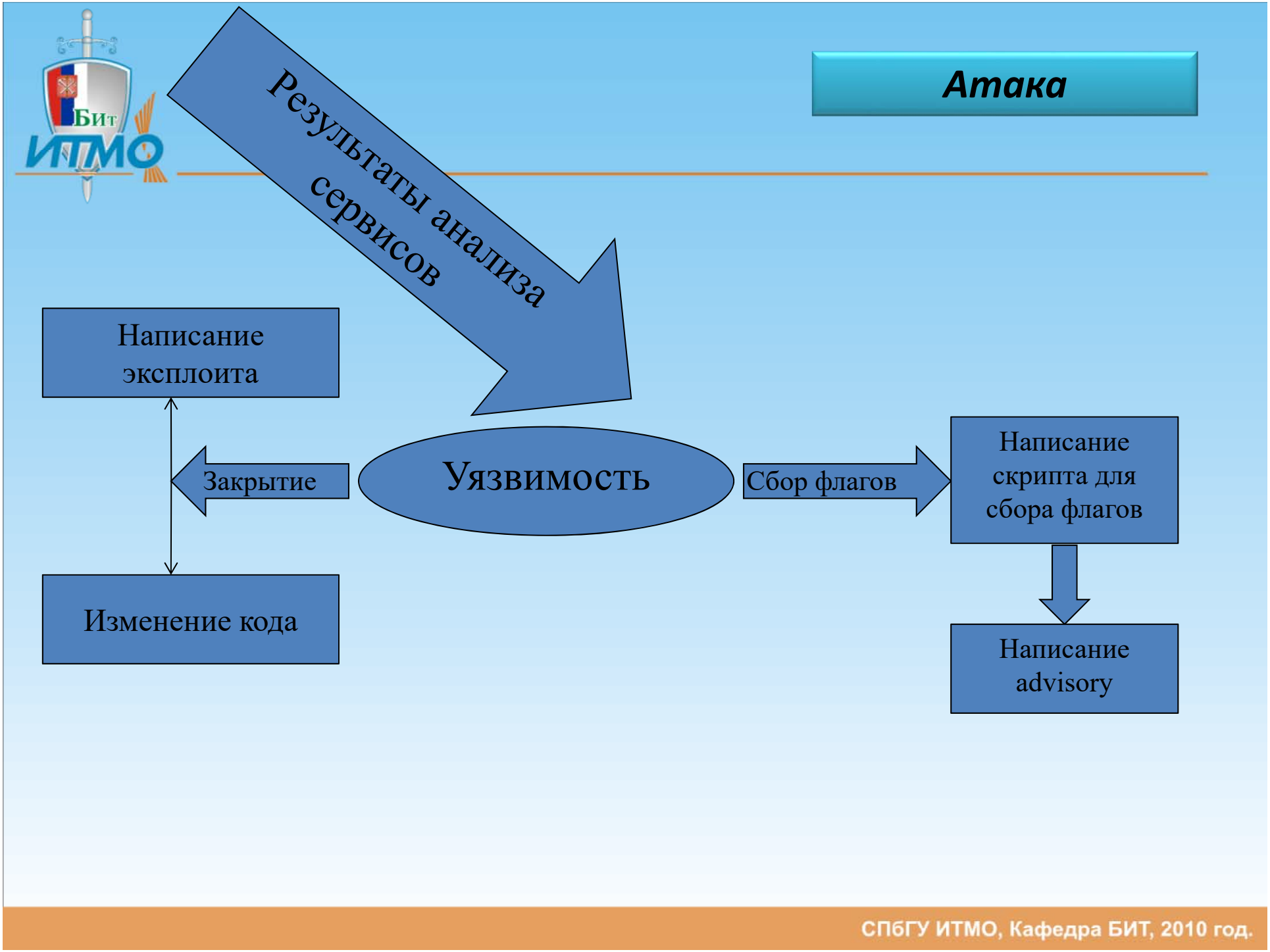

Predictable Resource Location
Brute Force
Buffer Overflow
Cross-site scripting
SQL Injection
OS Commandi ng
Insufficient Authenticat ion
Credential /Session Prediction
Weak Password Recovery Validation
Уязвимости

Структура команды

Капитан	Сетевой админ-р	Системный админ-р	Shell-кодер	Аналитик
Координация, мотивация, коммуникации	Настройка, поддержание функционирования каналов связи; мониторинг сетевого трафика	Функционирование сервера, сервисов, копирование и резервирование системы	Анализ исходного кода, написание эксплоитов, скриптов для сбора флагов и тд	Анализ бинарного кода на наличие уязвимостей
Организационные способности	Сетевые протоколы, маршрутизация	Архитектура ОС	Навык написания шелл-кода	Ассемблер, структура исполняемых файлов
	Wireshark, Snort	Системные инструменты и утилиты, бэкап-утилиты	Любимая среда разработки netcat	IDA Pro; Olly Dbg HIEW LordPE


До Начала
• Подготовка сети, серверов;
• Настройка VM, программ, средств мониторинга
Подготовительный этап (Стандартные процедуры)
Начало
• Расшифровка образа,
• запуск системы,
• смена пароля,
• проверка функционирования сервисов
Стартовый этап (Стандартные процедуры)
После начала
• Проверка открытых MySQL портов.
• Закрытие панелей администратора
• Chroot apache и тд.
Первоначальная защита (Стандартные процедуры)
Основная часть
Аналитическая работа, мозговой штурм, генерация идей
Соревновательная часть
СПбГУ ИТМО, Кафедра БИТ, 2010 год.


Защита
Мониторинг входящего/исходящего трафика
Снифинг файловой системы
Резервное копирование системы
Поиск файлов, разрещающих загрузку информации
Анализ на предмет XSS ссылок, форм ввода, форм регистрации
Просмотр передающихся сессий, cookies
Сервис
Проверка вложений во всех файлах
Закрытие уязвимостей по существующим advisory
Поиск бинарных файлов и их дизассемблирование
Анализ кода
Сканирование образа на наличие открытых портов


Атака
Результаты анализа сервисов
Написание эксплоита
Закрытие
Уязвимость
Сбор флагов
Написание скрипта для сбора флагов
Изменение кода
Написание advisory

Результаты **конференций**

- ❖Первоисточник информации о новых уязвимостях, угрозах и методах борьбы с ними;
- ❖Изучение методов защиты информации на практике молодыми специалистами (студентами);
- ❖Позитивная мотивация молодых специалистов, положительная ориентированность «кибернеформалов»;
- ❖Возможность с целью исследований производить взломы, атаки не нарушая закон;
- ❖Последующие изменения (улучшения) в оборудовании и программном обеспечении;
- ❖ Осведомленность специалистов в узкой области о проблемах других сфер информационной безопасности;
- ❖Формирование международного объединения IT-специалистов, специалистов по ИБ

Вывод – необходимость развития подобных мероприятий в России

RuCTF
ructf.ogr

UFO CTF

CITCTF
citctf.ifmo.ru

Спасибо за внимание!