

# JET SECURITY CONFERENCE



## VIII ежегодная конференция Центра информационной безопасности

1-2 июня 2017 года

[WWW.JET.SU](http://WWW.JET.SU)



# Секция Практическая безопасность

01

**АНДРЕЙ ЯНКИН**

Социо-техническая инженерия. Против взлома нет приема?

02

**КИРИЛЛ ЕРМАКОВ**

Security awareness на печальном опыте

03

**ПАВЕЛ ВОЛЧКОВ**

Honeypot – казаться, а не быть

04

**АРТЕМ АРТЕМОВ**

Расследование киберпреступлений

05

ВОПРОСЫ- ОТВЕТЫ



**JET** CONFERENCE

01/06/2017

# Социальная инженерия

Андрей Янкин, заместитель директора ЦИБ

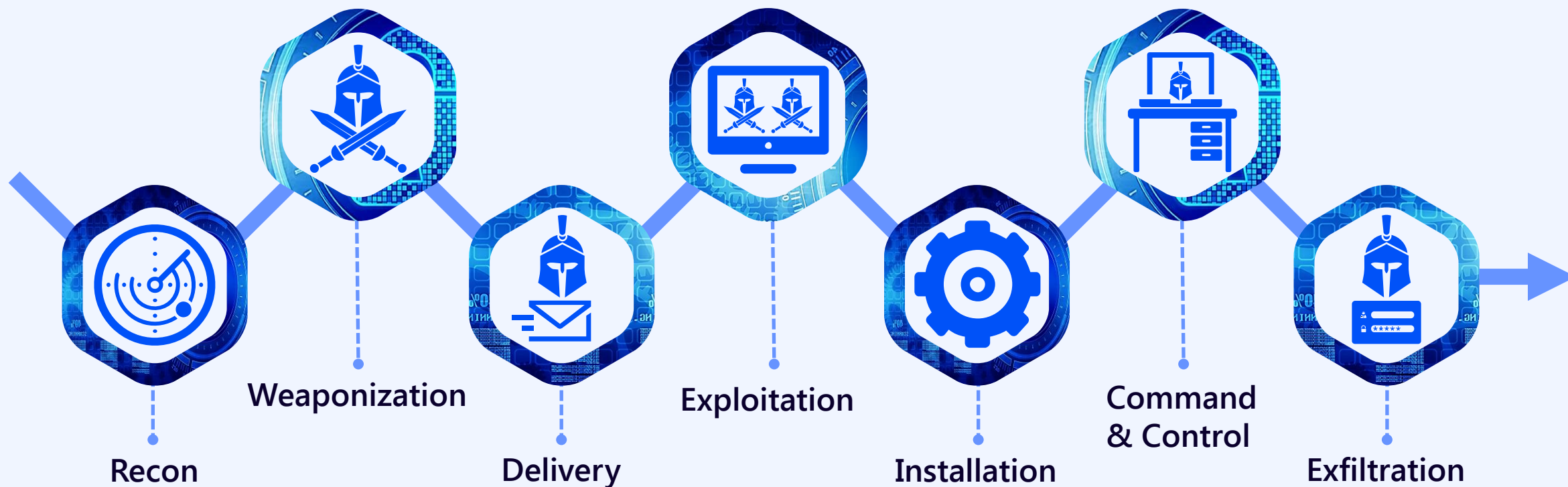


## Не баг, а фича





## Cyber Kill Chain



JET  
CONFERENCE

# Phishing



## Phishing

### Mass



### Spear



### Whaling



# Mass Phishing

Типовой сценарий в рамках пентеста:

- › Регистрация поддельных доменов
- › Сбор email-адресов
- › Пробные рассылки
- › Формирование писем
- › Массовая атака
- › Наперегонки с саппортом

Средний «пробой»: **5-7%**





# Spear Phishing

Типовой сценарий в рамках пентеста:

- › Изучение специфики работы компании
- › Поиск контактов жертв (HR, продажи,...)
- › Старт переписки, установка контакта
- › Заражение (возможно несколько итераций)



## Vishing

### Vishing = Voice Phishing

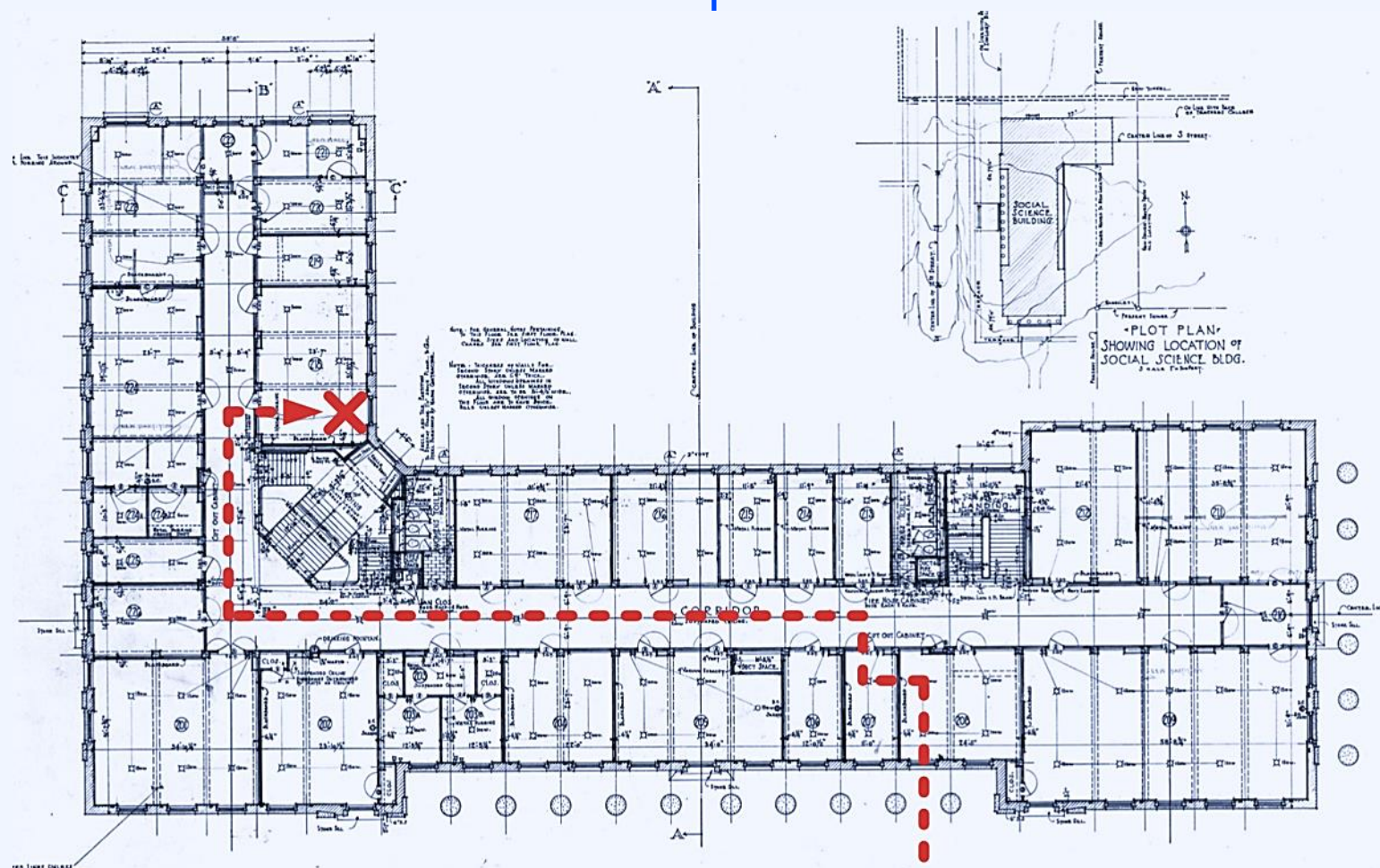
- Сбор информации
- Усиление других типов фишинга



# Дорожное яблоко



## Физическое проникновение



# Исследование мусора

**Dumpster Diving** – от dumpster –  
контейнер для мусора (от Dempster  
Dumpster – фирменного названия  
контейнера компании Dempster Brothers)





# Немного фантазии





# Социотехническая инженерия в пентесте

**WHY?**

- › Наиболее вероятная техника в рамках направленных и массовых атак
- › Осознание важности проблемы
- › Обучение пользователей

# Защита: обучение пользователей



# Защита: технические меры







**JET** CONFERENCE

01/06/2017

**ИНФОСИСТЕМЫ ДЖЕТ**

Спасибо за внимание!