3. Модель нарушителя

1	***Цель*** – желаемый результат на который направлен процесс деятельности нарушителя
2	***Мотивация*** - психофизиологический процесс, управляющий поведением человека, определяющий его направленность, организованность и активность
3	***Финансовое обеспечение*** – средства, позволяющие покрывать затраты, связанные с действиями нарушителя
4	***Техническое обеспечение*** – средства, позволяющие совершать запланированные действия нарушителю

Характеристики нарушителя

5	***Наличие и уровень профессиональной подготовки*** – определяет пригодность имеющихся у нарушителя навыков для достижения поставленной цели
6	***Наличие и качество предварительной подготовки*** – определяет качество планирования мероприятий по достижению поставленной цели
7	***Наличие и уровень внедрения на объект*** – определяет время и объем мероприятий необходимых для достижения поставленной цели

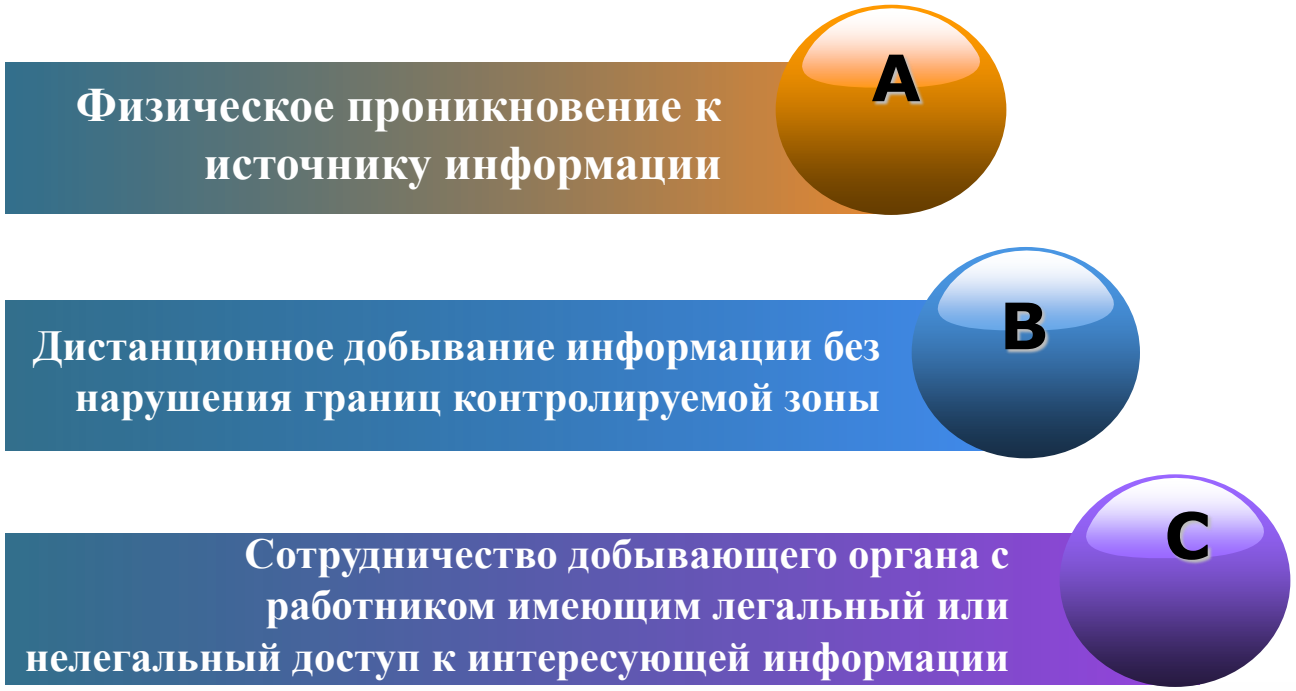
Классы нарушителей

А	действующие целенаправленно и обладающие практически неограниченным финансовым обеспечением (сотрудники иностранной разведки)
Б	действующие целенаправленно и обладающие ограниченным, но достаточно крупным финансовым обеспечением (конкурирующие организации, ОПГ и т.д.)
В	действующие целенаправленно, обладающие малым (или вообще отсутствующим) финансовым обеспечением, но имеющие хороший профессиональный уровень подготовки (криминальные группы)

Классы нарушителей

Г	действующие целенаправленно, обладающие малым (или вообще отсутствующим) финансовым обеспечением и имеющие низкий уровень профессиональной подготовки (сотрудники предприятий)
Д	действующие не целенаправленно (случайные люди)

Способы доступа нарушителя к носителю информации



Воздействие нарушителя

Воздействие

- **Преднамеренное**
- **Случайное**

Носитель

Угроза безопасности информации - **возможные воздействия на носитель информации приводящие к ущербу**

Характер угроз безопасности информации

Преднамеренный	Целенаправленные действия человека
Случайный	Не злонамеренные действия человека в силу его ***не компетентности***, усталости и т.д.

Исчисление ущерба

Количественное

ущерб исчисляется как стоимость товара в денежном эквиваленте, что ***позволяет его однозначно и точно осмыслить*** для принятия последующего решения по минимизации ущерба

Качественное

ущерб исчисляется в виде некоторой условной категории (высокий, средний, низкий). Такая оценка является ***субъективной и сложной для осмысления***

Виды угроз безопасности информации

Конфиденциальности	Нарушение свойства информации быть известной только определенным субъектам (создатель, обладатель)
Целостности	Изменение содержания (искажение), уничтожение информации
Доступности	Нарушаются доступ к информации, работоспособность носителя

Виды угроз безопасности информации

Подлинности	приводит к невозможности однозначно идентифицировать (определить) автора или источник, откуда она получена
Сохранности	ее следствием является не возможность обеспечить такой режим хранения информации, который позволял бы гарантировать ее конфиденциальность, целостность и доступность

Источники угроз

Человек	его действия могут носить целенаправленный или случайный характер приводящие к утечке информации
Технические средства	выход из строя (не работоспособность) приводит к не возможности обработки информации и утрате информации, которая хранилась или обрабатывалась таким средством. Могут содержать недокументированные возможности приводящие к утечке информации
Программное обеспечение	может содержать недокументированные возможности приводящие к утечке информации. Вредоносные программы позволяют реализовать угрозы безопасности информации

Источники угроз

Внешняя среда	природные стихийные бедствия (молнии, наводнения) могут быть причиной потери сведений (выход из строя оборудования, повреждение системы электропитания)

Утечка информации

Разглашение

Человек получивший доступ к информации может преднамеренно или случайно ее передать третьему лицу

Утечка информации

Утечка информации по техническим каналам

Перехват информации выполняется дистанционно без проникновения в контролируемую зону

Утечка информации

Несанкционированный доступ к информации

Реализуется при доступе нарушителя к информации в информационной системе

Кибератака

Кибератака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

Концепция информационной безопасности Республики Беларусь (Постановление Совета безопасности Республики Беларусь №1 от 18.03.2019)

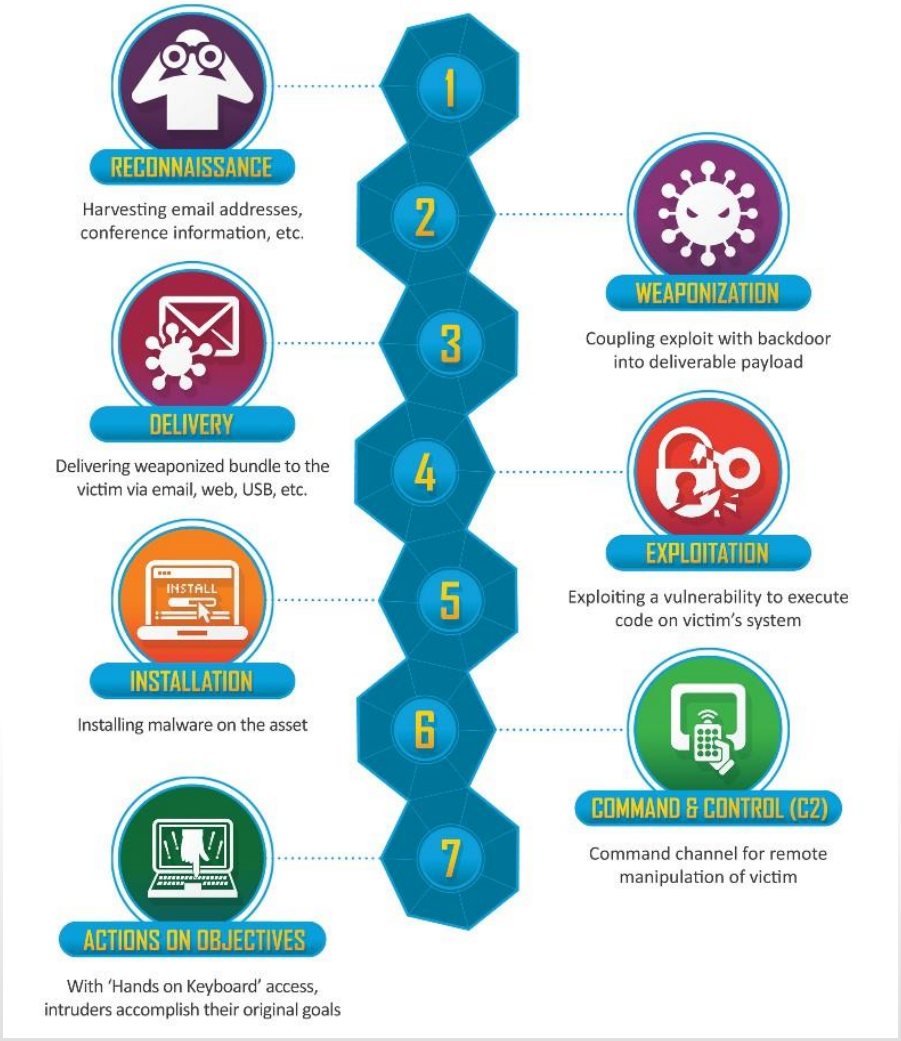
Объекты на которые осуществляются кибератаки

1	устройства (компьютеры и т.д.) пользователей, серверы
2	оборудование используемое для организации каналов связи (коммутаторы, маршрутизаторы)

Последствия кибератаки

1	нарушение или прекращение функционирования объектов информационной инфраструктуры
2	создание угрозы безопасности информации

Модель нарушителя Cyber-Kill Chain



LOCKHEED MARTIN

Особенности модели

1. Последовательная реализация первых шести этапов позволяет нарушителю скомпрометировать хотя бы один хост в информационной системе (ИС)
2. Седьмой этап заключается в развитии атаки в самой корпоративной сети (горизонтальной плоскости) со скомпрометированного хоста

Open source intelligence – OSINT (разведка на основе открытых источников)

1

OSINT

сбор информации о информационной системе (ИС), в том числе из открытых источников. Одна из важнейших целей - обнаружение уязвимостей

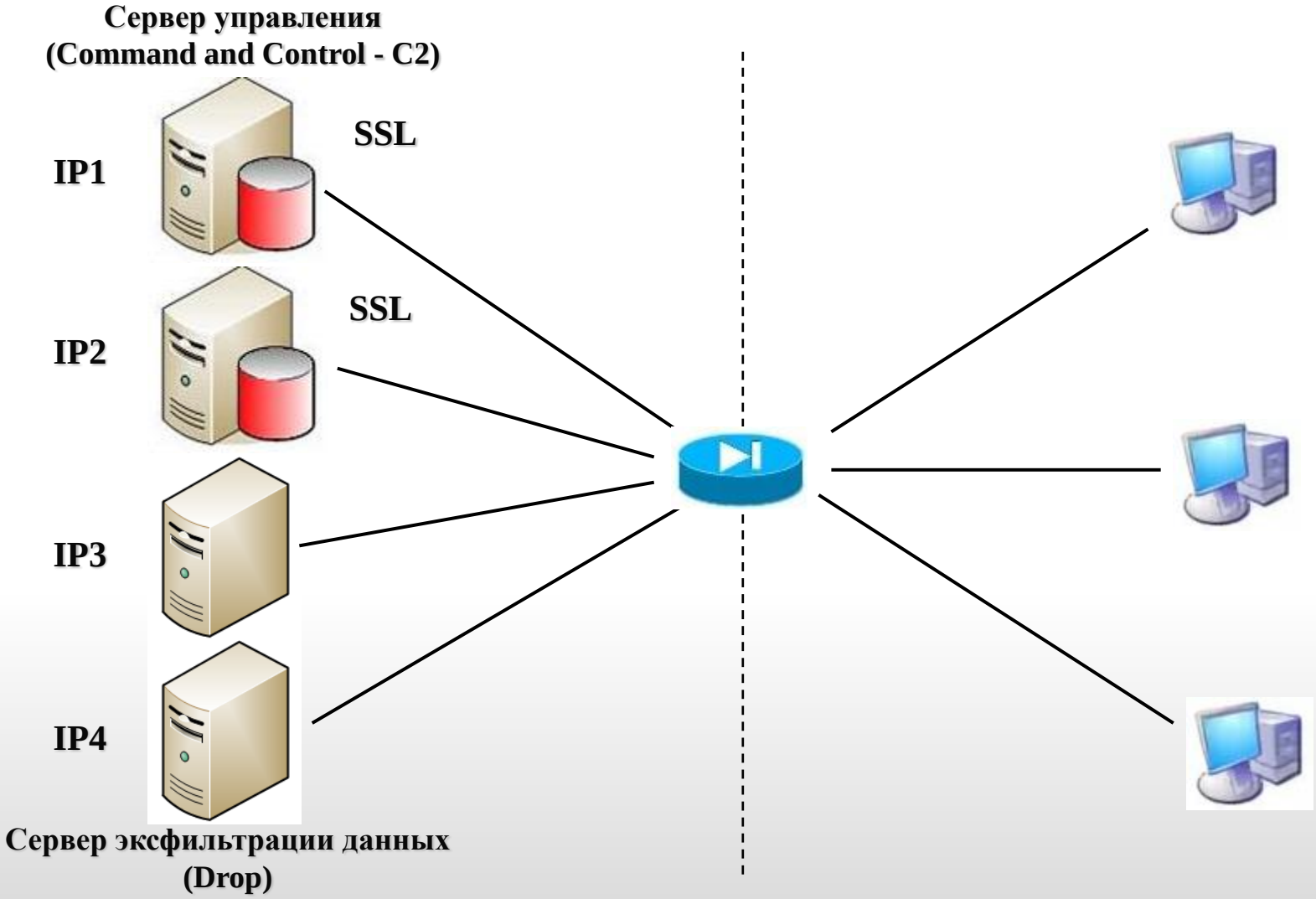
Weaponization (вооружение)

2

Вооружение

подготовка (разработка или покупка) «инструментов» для эксплуатации уязвимостей (exploit), вредоносных программ (malware), и их упаковка, подготовка инфраструктуры (C2 & Drop Servers, SSL certificates)

Инфраструктура нарушителя



Инфраструктура нарушителя

C2 сервер	Позволяет скрыть адресацию нарушителя. На них размещаются подготовленные нарушителем SSL сертификаты. Подключение к C2 организуется методом Reverse Shell
DROP сервер	Используется нарушителем для выгрузки данных из скомпрометированной ИС
SSL сертификат	Сертификат для установления TLS соединения

Delivery (доставка)

3

Доставка

фишинг; целенаправленный фишинг; атака на цепочку поставок; атака «водопой»

Фишинг

Фишинг (phishing)

(выуживание идентификаторов) – способ получения идентификаторов пользователя информационных систем нарушителем, который основан на предоставлении пользователю такой информации и создании нарушителем таких условий ее восприятия, при которых пользователь примет ошибочное решение и в результате чего выполнит некоторое действие, которое является выгодным нарушителю

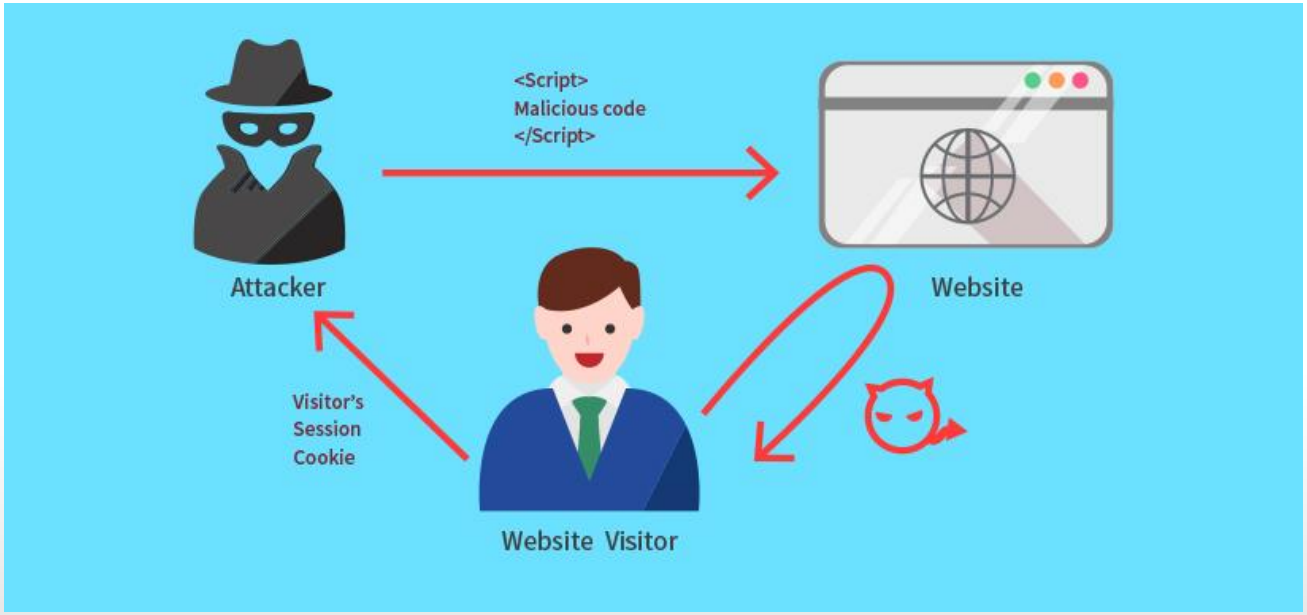
Действия, совершаемые пользователем и выгодные нарушителю

1. **Передача идентификаторов (логин, пароль) пользователем**
2. **Загрузка вредоносной программы на компьютер пользователя**

Атака на цепочку поставок (Supply Chain Attack)

Атака «водопой» (Watering Hole Attack)

Получение информации об информационных ресурсах посещаемых пользователем → **Внедрение вредоносного кода в титульную страницу сайта** → **Посещение сайта с вредоносным кодом**



Exploitation (эксплуатация)

4

Эксплуатация

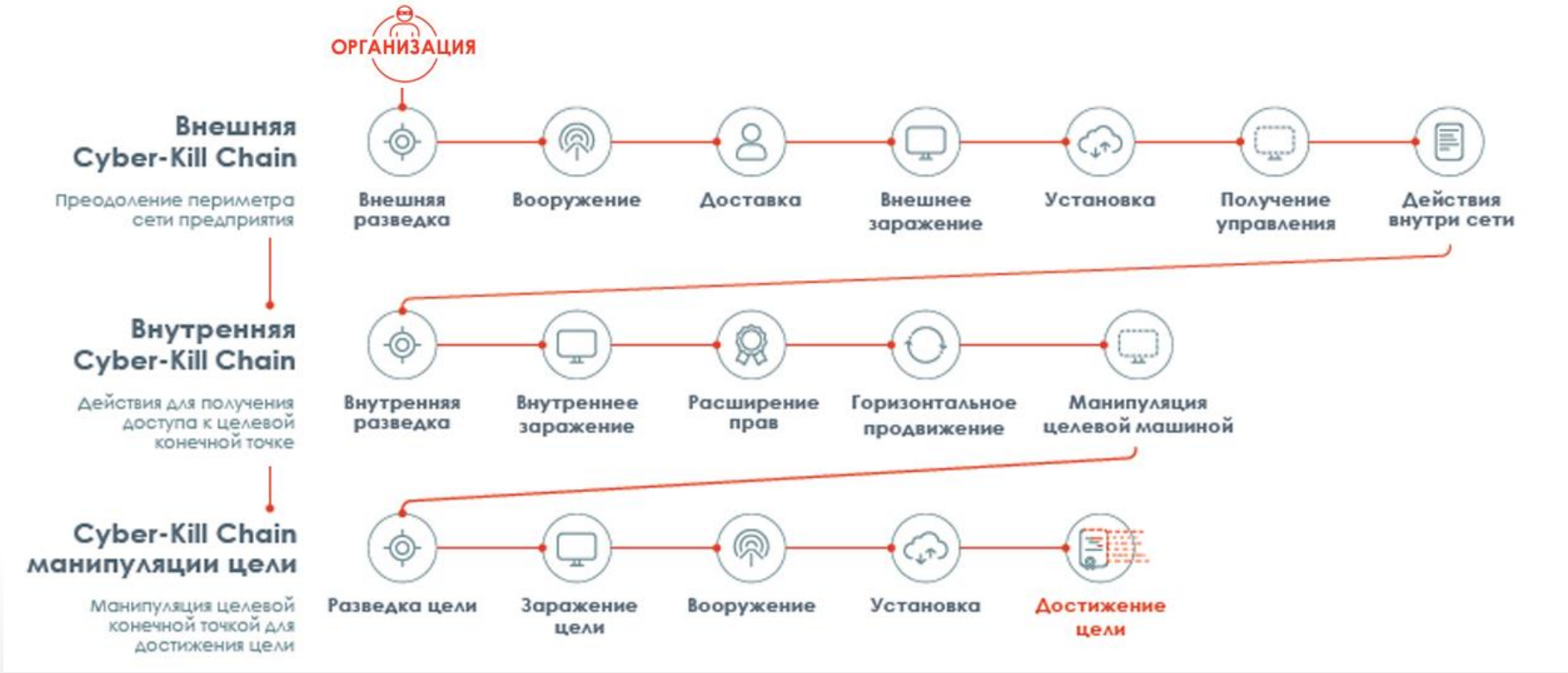
1. Обеспечение корневых полномочий;
2. Установка TLS соединения для загрузки вредоносной программы с последующей ее распаковкой

Cyber Kill Chain

5 **Установка** — Инсталляция вредоносной программы

6 **Получение управления** — Вредоносная программа подключается к серверу управления (C2) нарушителя и ждет команд

Действия нарушителя внутри ИС



Действия нарушителя внутри ИС