

< Teach  
Me  
Skills />

# Mitre Att&ck

Типы атак II

# Вопросы по предыдущим темам или ДЗ

# Mini-quizе по прошлым темам:

1. **Какие существуют тактики для закрепления ПО в системе?**
2. **Зачем существует матрица Mitre?**
3. **Какие основные пункты к СКС?**
4. **Что такое кейлоггинг?**
5. **Какие виды Reconnaissance (Разведка) существуют?**

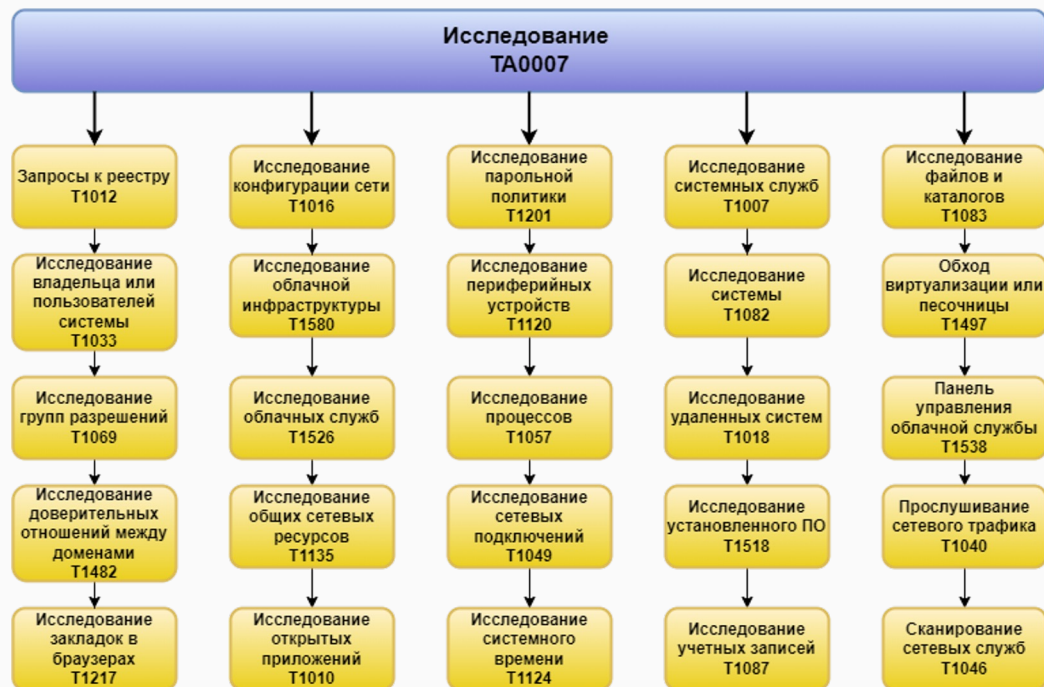
# Mini-quiz по новой теме:

1. **Какие, как вы думаете, еще существуют матрицы Mitre по аналогии с матрицей атакующих?**
2. **Что вредного могут сделать злоумышленники по отношению к инфраструктуре?**
3. **Как можно защититься от атаки?**
4. **Как необходимо реагировать на атаку?**
5. **Где хранятся логи систем Win/Unix?**

# План занятия

1. Разберем остальные матрицы **Mitre**
2. Изучим оставшиеся тактики и техники злоумышленников
3. Разберем несколько инцидентов при помощи матрицы **Mitre Att&ck**
4. Придумаем возможные способы защиты от этих атак при помощи матрицы **Defend**
5. Разработаем план реагирования на инцидент при помощи матрицы **Re&ct**

**Discovery(исследование)** - состоит из методов, которые злоумышленник может использовать для получения знаний о системе и внутренней сети.



# Lateral movement

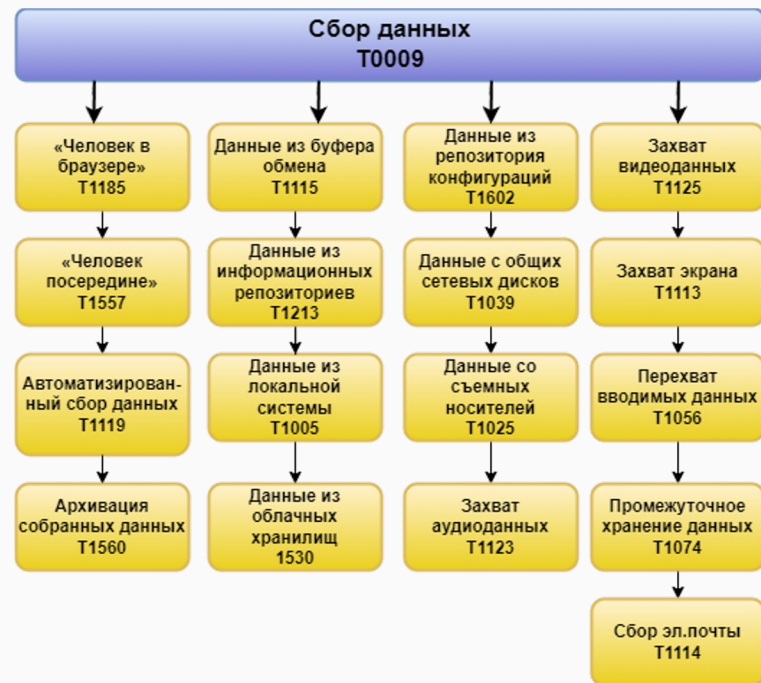
**Lateral movement (перемещение внутри периметра)** - состоит из методов, которые злоумышленники используют для входа и управления удаленными системами в сети.





# Collection

**Collection (сбор данных)** - состоит из методов, которые злоумышленники могут использовать для сбора информации, и источников, из которых собирается информация, имеющая отношение к достижению целей.





# Command & Control

**Command & Control (управление и контроль) –**

состоят из методов, которые злоумышленники могут использовать для связи с системами, находящимися под их контролем в сети жертвы.



# Exfiltration

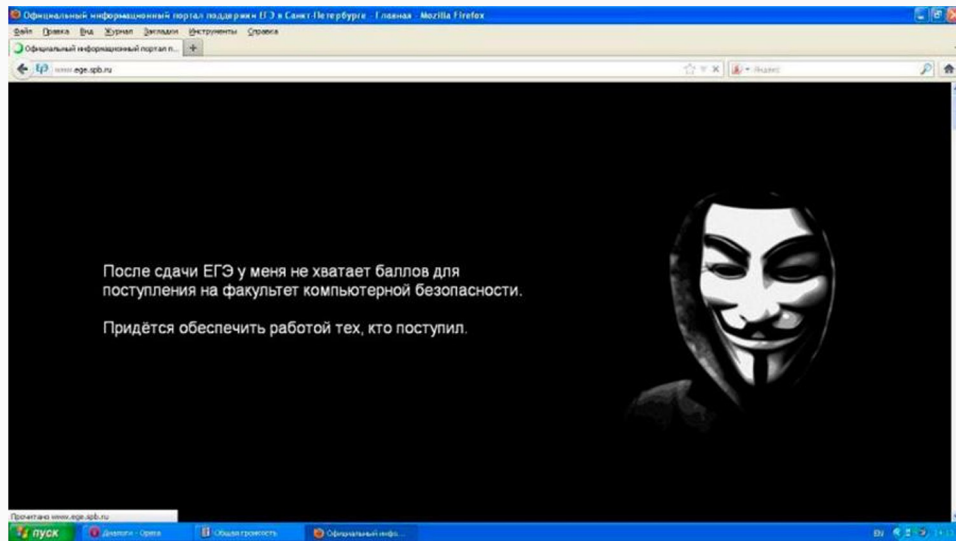
**Exfiltration (Эксфильтрация данных)** - состоит из методов, которые злоумышленники могут использовать для кражи данных из вашей сети.



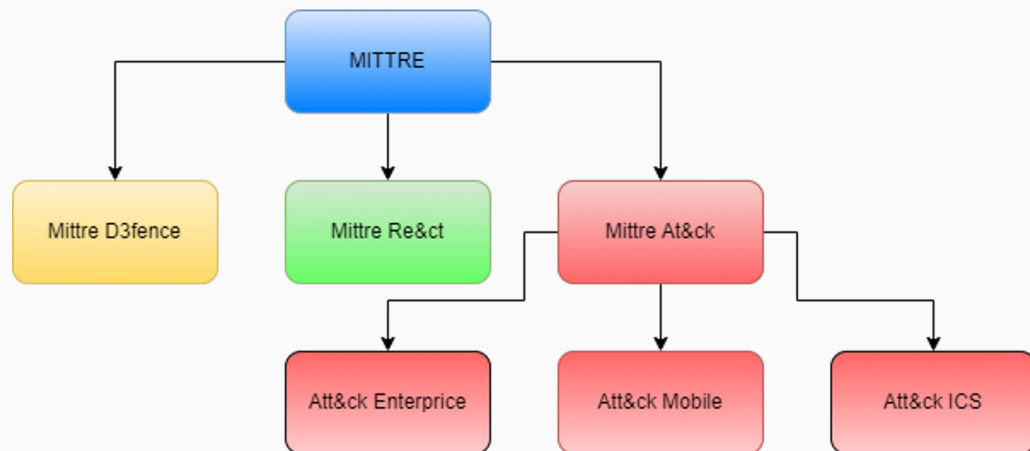
**Эксфильтрация, или экстракция — тактика перемещения персонала с территории, находящейся под контролем противника, и доставки в безопасную зону.**

# Impact

**Impact (воздействие)** - состоит из методов, которые злоумышленники используют для нарушения доступности или нарушения целостности путем манипулирования бизнес-процессами и операционными процессами.

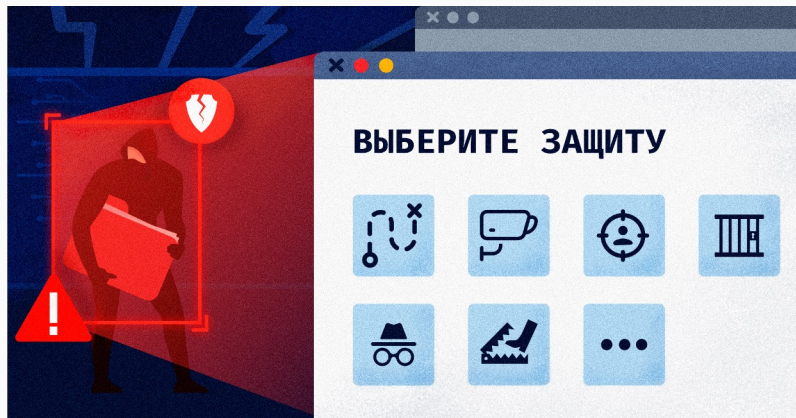


### Примерная структура матриц Mitre



# Mitre D3fend

**D3fend** – база, матрица, которая содержит структурированный набор техник для обеспечения контрмер.



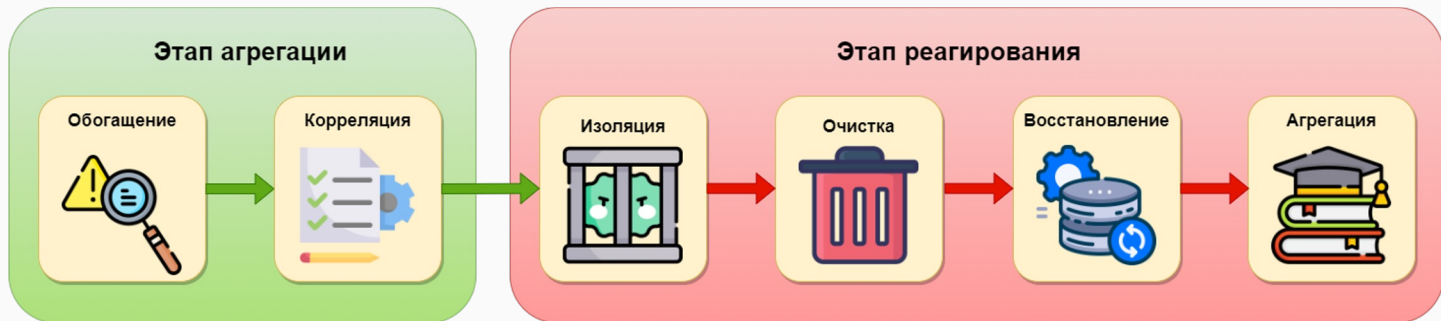
ATTACK Lookup										D3FEND Lookup							
Тактики																	Категории
Harden				Detect					Isolate			Deceive		Evict			
Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	Process Eviction	
Dead Code Elimination	Certificate Pinning	Message Authentication	Disk Encryption	Dynamic Analysis	Homograph Detection	Sender MTA Separation Analysis	Administrative Network Activity Analysis	Firmware Verification	Database Query String Analysis	Authentication Event Thresholding	Hardware-based Process Isolation	Broadcast Domain Isolation	Connected Honeynet	Decoy File	Account Locking	Process Termination	
Exception Handler Pointer Validation	Multi-factor Authentication	Message Encryption	Driver Load Integrity Checking	Emulated File Analysis	URL Analysis	Sender Reputation Analysis	Certificate Analysis	Operating System Monitoring	File Access Pattern Analysis	Authorization Event Thresholding	Encrypted Traffic Filtering	Encrypted Tunnels	Integrated Honeynet	Decoy Network Resource	Authentication Cache Invalidation		
Process Segment Execution Prevention	One-time Password	Transfer Agent Authentication	RF Shielding	File Content Rules	File Hashing	Active Certificate Analysis	Endpoint Health Beacon	Input Device Analysis	Indirect Branch Call Analysis	Mandatory Access Control	Executable Denial	Inbound Traffic Filtering	Standalone Honeynet	Decoy Persona			
Segment Address Offset Randomization	Strong Password Policy		TPM Boot Integrity	Bootloader Authentication		Passive Certificate Analysis	Local Account Monitoring	Process Code Segment Verification	Resource Access Pattern Analysis	Executable Denial	Outbound Traffic Filtering	DNS Abusing		Decoy Public Release			
Stack Frame Canary Verification			Software Update			Client-server Payload Profiling	Memory Boundary Tracking	Process Self-Modification Detection	User Data Transfer Analysis	Executable Denial	DNS Denial			Decoy Session Token			
Pointer Authentication						DNS Traffic Analysis	Scheduled Job Analysis	Process Spawning Analysis	User Credential Logon Pattern Analysis	Executable Denial	Forward Resolution Domain Denial			Decoy User Credential			
						File Carving	System Daemon Monitoring	Process Lineage Analysis	Web Session Activity Analysis	Script Execution Analysis	Shadow Back Comparisons						
						IPC Traffic Analysis	Network Traffic Community Deviation	System File Analysis	Per Host Download/Upload Ratio Analysis								

**Реагирование на инциденты** (Incident Response, **IR**) — комплекс мероприятий по обнаружению и прекращению кибератаки или утечки данных из инфраструктуры организации. Так же включает в себя действия по устранению последствий.

## Схема

Фреймворк создан для сбора, описания и классификации опасных техник реагирования на аварии.

Общее представление о реагировании на компьютерные инциденты



# STIX

[Структурированное выражение информации](#) об угрозах (STIX™) — это язык и формат сериализации, используемый для обмена информацией о киберугрозах (CTI).





# TIP платформы

**Kaspersky**

**Threat Intelligence Portal**



**MISP**  
Threat Sharing

[ссылка](#)

[установка MISP](#)

Основное задание:

Вы – хакер находящийся в интернете, вам необходимо проникнуть внутрь инфраструктуры и скопроментировать 2 цели.

1-ая компьютер глав буха компании

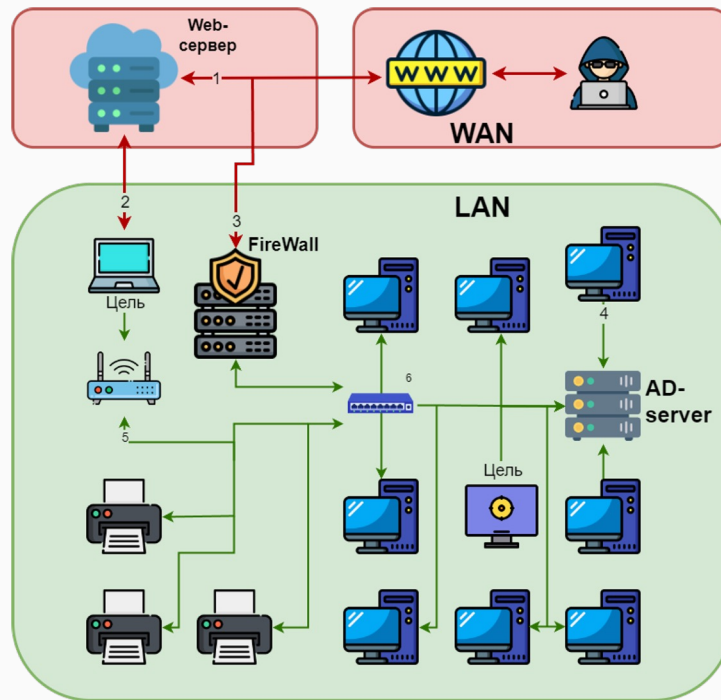
2-ая ноутбук системного администратора.

Применяя матрицу Att&ck.

**\*Задание:**

Необходимо разработать план защиты и план реагирования на атаку, которую вы провели гипотетически в предыдущем задании.

Используя матрицы D3fence и Re&ct



**Схема атакуемой инфраструктуры**