


CISCO  
SECURE

 CISCO The bridge to possible

# ОСНОВНЫЕ СЦЕНАРИИ РЕАЛИЗАЦИИ УГРОЗ НА АСУ ТП

## И ИХ ПРЕЛОМЛЕНИЕ НА МЕТОДИКУ ОЦЕНКИ УГРОЗ ФСТЭК

Алексей Лукацкий

Бизнес-консультант по безопасности

[alukatsk@cisco.com](mailto:alukatsk@cisco.com)



# Как совершаются атаки?

Исключений не бывает

- ❑ **Никогда** атака не является точечным действием и всегда состоит из ряда связанных между собой шагов
- ❑ Отражение/нейтрализация атак могут осуществляться на любом этапе и пропуск первых этапов не означает провал ИБ
- ❑ Ключевой задачей ИБ является мониторинг различных этапов совершения атаки и блокирование самого важного из них, ради которого злоумышленник все и затевал

# Из каких этапов состоит атака?

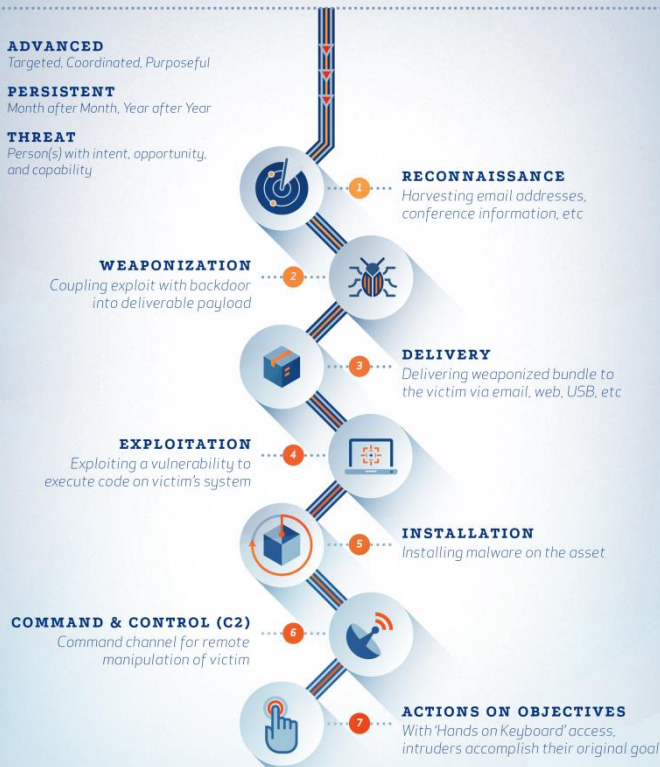
Сама идея не нова, но оформлена она была компанией Lockheed Martin



## CYBER KILL CHAIN®

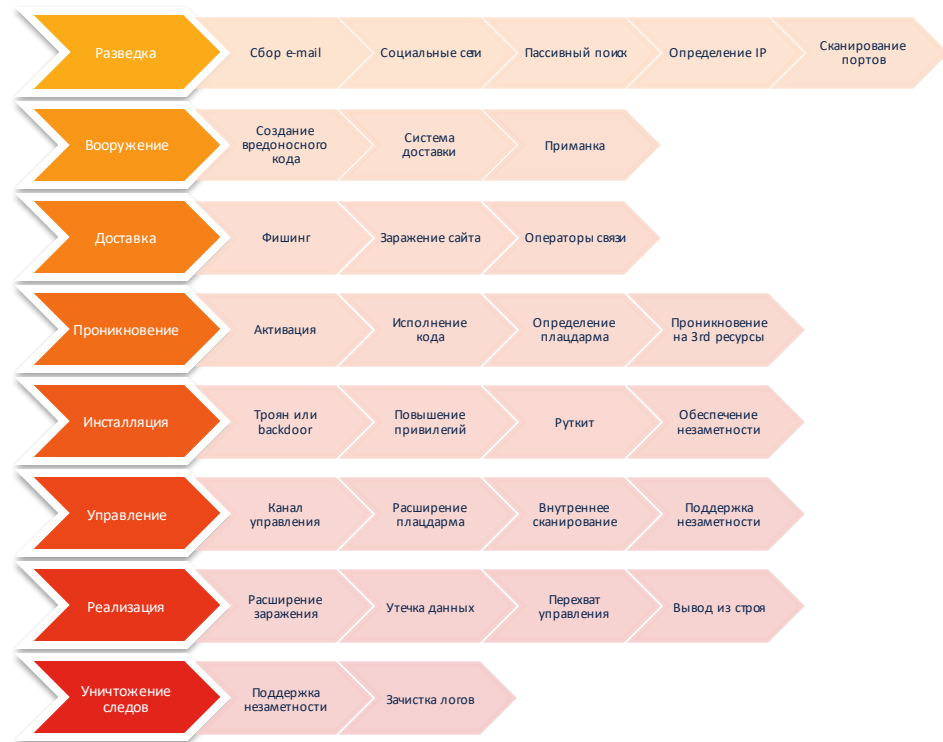
Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

- A : ADVANCED**  
*Targeted, Coordinated, Purposeful*
- P : PERSISTENT**  
*Month after Month, Year after Year*
- T : THREAT**  
*Person(s) with intent, opportunity, and capability*



# Стандартный набор шагов злоумышленника

Многие термины взяты из документов американского МинОбороны



# Этап 1: корпоративная сеть



# Старый, но показательный пример: BlackEnergy

- Направленный фишинг
  - Документ Word и PowerPoint с макросом
  - Тематические рассылки на тему нефтянки
- Использование ODay для Windows
- Разработка и использование ICS эксплойт для HMI



## Этап 2: промышленная сеть



# Как попасть из пункта А в пункт Б?



Определение текущих  
доверенных соединений

Манипуляции  
окружением

*Использование  
административных  
привилегий для установления  
новых соединений*

Физические элементы  
*USB, CD, инсайдер, устройства*

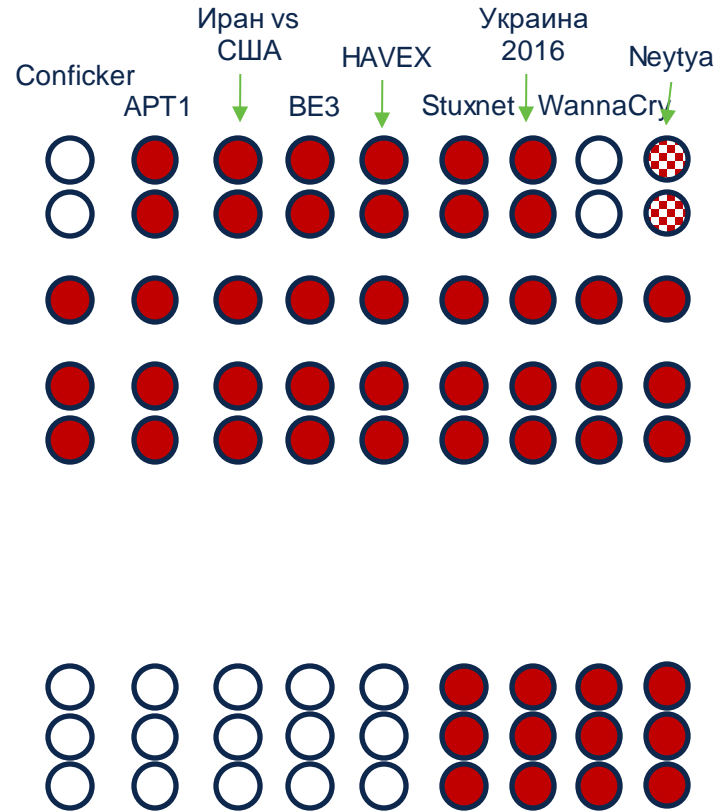
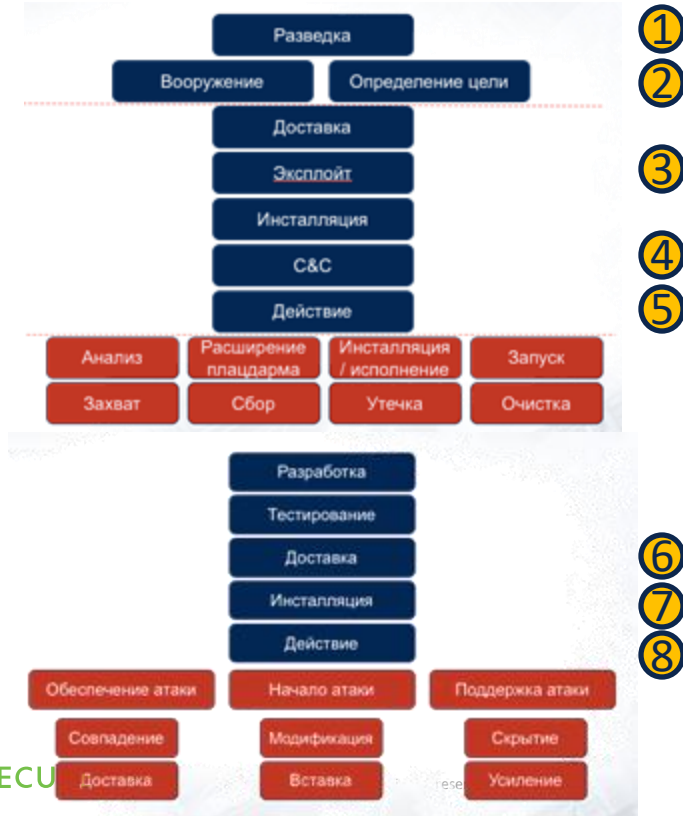




# Как попасть с 1-го этапа на 2-й

- Доверенные соединения (historians)
- Доступ от производителей
- Удаленный доступ персонала
- Резервные копии и иные задачи по репликации
- Коммуникации системного управления (патчи, мониторинг, конфигурации и др.)
- Доступ к серверам хранения исторической информации
- Доступ через dialup или Wi-Fi
- Waterholing
- Социальный инжиниринг
- Закладки в оборудование
- Флешки и иные носители информации
- Возможно еще что-то

# Промежуточный итог



# Каждый шаг может быть реализован по-разному

Поэтому концепция kill chain – это только начало истории



- Каждый шаг в цепочке действий злоумышленников реализуется десятками различных способов (техник)
- Разные хакерские группировки используют разные техники
- Техники постоянно эволюционируют и реализуются с помощью разного ПО или команд или процессов или действий

# Множество разных попыток описать действия хакеров

Есть даже Unified Kill Chain

| #  | Unified Kill Chain   | Cyber Kill Chain® (CKC) | Laliberte | Nachreiner | Bryant | Malone | MITRE ATT&CK™ | UKC after literature study | UKC after Red Team C1 | UKC after Red Team C2 | UKC after Red Team C3 | UKC after Red Team KC | UKC after APT28 C4 & KC |
|----|----------------------|-------------------------|-----------|------------|--------|--------|---------------|----------------------------|-----------------------|-----------------------|-----------------------|-----------------------|-------------------------|
| 1  | Reconnaissance       | 1                       | 1         | 1          | 1      | 1      |               | 1                          | 1                     | 1                     | 1                     | 1                     | 1                       |
| 2  | Weaponization        | 2                       | 3         | 3          | 3      | 2      |               | 2                          | 2                     | 2                     | 2                     | 2                     | 2                       |
| 3  | Delivery             | 3                       | 5         | 5          | 6      | 3      |               | 7                          | 7                     | 3                     | 3                     | 3                     | 3                       |
| 4  | Social Engineering   | 5                       | 6         | 6          | 11     | 5      |               | 3                          | 3                     | 4                     | 4                     | 4                     | 4                       |
| 5  | Exploitation         | 6                       | 8         | 8          | 14     | 6      |               | 5                          | 4                     | 5                     | 5                     | 5                     | 5                       |
| 6  | Persistence          | 8                       | 14        | 9          | 18     | 8      | 6             | 6                          | 5                     | 6                     | 6                     | 6                     | 6                       |
| 7  | Defense Evasion      | 18                      | 18        | 14         | 16     | 10     | 11            | 8                          | 6                     | 7                     | 7                     | 7                     | 7                       |
| 8  | Command & Control    |                         |           | 18         |        | 5      | 7             | 9                          | 8                     | 8                     | 8                     | 8                     | 8                       |
| 9  | Pivoting             |                         |           |            |        | 11     | 13            | 11                         | 9                     | 9                     | 9                     | 9                     | 9                       |
| 10 | Discovery            |                         |           |            |        | 14     | 10            | 10                         | 11                    | 11                    | 11                    | 10                    | 10                      |
| 11 | Privilege Escalation |                         |           |            |        | 17     | 14            | 14                         | 10                    | 10                    | 10                    | 11                    | 11                      |
| 12 | Execution            |                         |           |            |        | 18     | 12            | 12                         | 14                    | 14                    | 14                    | 12                    | 12                      |
| 13 | Credential Access    |                         |           |            |        |        | 15            | 13                         | 12                    | 12                    | 12                    | 13                    | 13                      |
| 14 | Lateral Movement     |                         |           |            |        |        | 16            | 17                         | 13                    | 13                    | 13                    | 14                    | 14                      |
| 15 | Collection           |                         |           |            |        |        | 8             | 15                         | 17                    | 17                    | 17                    | 17                    | 15                      |
| 16 | Exfiltration         |                         |           |            |        |        |               | 16                         | 15                    | 15                    | 15                    | 15                    | 16                      |
| 17 | Target Manipulation  |                         |           |            |        |        |               |                            | 16                    | 16                    | 16                    | 16                    | 17                      |
| 18 | Objectives           |                         |           |            |        |        |               |                            |                       |                       |                       |                       | 18                      |

# ATT&CK: база знаний поведения хакеров

Adversarial  
Tactics  
Techniques  
&  
Common  
Knowledge

“ MITRE начала этот проект в 2013, документируя тактики, техники и процедуры (TTP), которые использовались в целевых атаках против сетей на базе Windows. ”



# Элементы АТТ&СК®



1. Матрица
2. Платформа
3. ТТР
4. Группы
5. Программное обеспечение
6. Меры защиты



# Матрица АТТ&СК

Технологические домены: что вы защищаете

Платформы

## ▶ Enterprise

Windows      Linux  
macOS        Cloud

- NEW** Сетевые устройства
- NEW** PRE-АТТ&СК включена

## ▶ Mobile

Android  
iOS

## ▶ ICS

АСУ ТП

- Контролирующий сервер
- Инженерные рабочие станции
- Контроллер
- HMI
- Сервера ввода/вывода
- Системы ПАЗ

| 1                                      | 2                             | 3                                   | 4                                     | 5                                        | 6                                        | 7                                       | 8                                       | 9                                      | 10                                        | 11                                     | 12                                    | 13                                    | 14                            |
|----------------------------------------|-------------------------------|-------------------------------------|---------------------------------------|------------------------------------------|------------------------------------------|-----------------------------------------|-----------------------------------------|----------------------------------------|-------------------------------------------|----------------------------------------|---------------------------------------|---------------------------------------|-------------------------------|
| Reconnaissance                         | Resource Development          | Initial Access                      | Execution                             | Persistence                              | Privilege Escalation                     | Defense Evasion                         | Credential Access                       | Discovery                              | Lateral Movement                          | Collection                             | Command and Control                   | Exfiltration                          | Impact                        |
| 10 techniques                          | 6 techniques                  | 9 techniques                        | 10 techniques                         | 18 techniques                            | 12 techniques                            | 37 techniques                           | 14 techniques                           | 25 techniques                          | 9 techniques                              | 17 techniques                          | 16 techniques                         | 9 techniques                          | 13 techniques                 |
| Active Scanning (2)                    | Acquire Infrastructure (4)    | Drive-by Compromise                 | Command and Scripting Interpreter (8) | Account Manipulation (4)                 | Abuse Elevation Control Mechanism (4)    | Abuse Elevation Control Mechanism (4)   | Brute Force (4)                         | Account Discovery (4)                  | Exploitation of Remote Services           | Archive Collected Data (3)             | Application Layer Protocol (4)        | Automated Exfiltration (1)            | Account Access Removal        |
| Gather Victim Host Information (4)     | Compromise Accounts (2)       | Exploit Public-Facing Application   | Explanation for Client Execution      | BITS Jobs                                | Access Token Manipulation (5)            | Access Token Manipulation (5)           | Credentials from Password Stores (3)    | Application Window Discovery           | Internal Spearphishing                    | Audio Capture                          | Communication Through Removable Media | Data Transfer Size Limits             | Data Destruction              |
| Gather Victim Identity Information (3) | Compromise Infrastructure (4) | External Remote Services            | Inter-Process Communication (2)       | Boat or Lagon Autostart Execution (12)   | Access Taken Manipulation (5)            | Access Taken Manipulation (5)           | Exploitation for Credential Access      | Browser Bookmark Discovery             | Lateral/Target Transfer                   | Automated Collection                   | Automated Removable Media             | Data Encrypted for Impact             | Data Encrypted for Impact     |
| Gather Victim Network Information (4)  | Develop Capabilities (4)      | Hardware Additions                  | Native API                            | Boat or Lagon Initialization Scripts (5) | Boat or Lagon Autostart Execution (12)   | Deobfuscate/Decode Files or Information | Forced Authentication                   | Cloud Infrastructure Discovery         | Remote Service Session Hijacking (2)      | Clipboard Data                         | Data Obfuscation (3)                  | Data Manipulation (3)                 | Data Manipulation (3)         |
| Gather Victim Org Information (4)      | Establish Accounts (2)        | Phishing (3)                        | Scheduled Task/Job (6)                | Browser Extensions                       | Boat or Lagon Initialization Scripts (5) | Direct Volume Access                    | Input Capture (4)                       | Cloud Service Dashboard                | Remote Services (4)                       | Data from Cloud Storage Object         | Dynamic Resolution (3)                | Defacement (2)                        | Defacement (2)                |
| Phishing for Information (3)           | Obtain Capabilities (6)       | Replication Through Removable Media | Shared Module                         | Compromise Client Software Binary        | Create or Modify System Process (4)      | Explanation for Defense Evasion         | Man-in-the-Middle (2)                   | Cloud Service Discovery                | Replication Through Removable Media       | Data from Configuration Repository (2) | Encrypted Channel (2)                 | Exfiltration Over C2 Channel          | Exfiltration Over C2 Channel  |
| Search Closed Sources (2)              | Trusted Relationship          | Supply Chain Compromise (3)         | Software Deployment Tools             | Event Triggered Execution (15)           | Event Triggered Execution (15)           | Execution Guardrails (1)                | Modify Authentication Process (4)       | File and Directory Discovery           | Software Deployment Tools                 | Data from Information Repositories (2) | Fallback Channels                     | Exfiltration Over Physical Medium (1) | Firmware Corruption           |
| Search Open Technical Databases (5)    | Valid Accounts (4)            | Windows Management Instrumentation  | System Services (2)                   | Create Account (3)                       | Exploitation for Privilege Escalation    | EvilWinRM (1)                           | Network Sniffing                        | Network Service Scanning               | Taint Shared Content                      | Data from Local System                 | Ingress Toot Transfer                 | Exfiltration Over Web Service (2)     | Inhibit System Recovery       |
| Search Open Websites/Domains (2)       |                               |                                     | User Execution (2)                    | Create or Modify System Process (4)      | Group Policy Modification                | Group Policy Modification               | OS Credential Dumping (8)               | Network Share Discovery                | Use Alternate Authentication Material (4) | Data from Network Shared Drive         | Multi-Stage Channels                  | Exfiltration Over Web Service (2)     | Network Denial of Service (2) |
| Search Victim-Owned Websites           |                               |                                     | External Remote Services              | Event Triggered Execution (15)           | Hijack Execution Flow (11)               | Hijack Execution Flow (11)              | Steel Application Access Taken          | Network Sniffing                       |                                           | Data from Removable Media              | Non-Application Layer Protocol        | Scheduled Transfer                    | Resource Hijacking            |
|                                        |                               |                                     | Hijack Execution Flow (11)            | Process Injection (11)                   | Scheduled Task/Job (4)                   | Scheduled Task/Job (4)                  | Steel or Forge Kerberos Tickets (4)     | Peripheral Device Discovery            |                                           | Data from Removable Media              | Non-Standard Port                     | Transfer Data to Cloud Account        | System Shutdown/Reboot        |
|                                        |                               |                                     | Implant Container Image               | Valid Accounts (4)                       | Office Application Startup (6)           | Office Application Startup (6)          | Two-Factor Authentication Interception  | Permission Groups Discovery (3)        |                                           | Data Staged (2)                        | Protocol Tunneling                    |                                       |                               |
|                                        |                               |                                     | Pre-OS Boot (5)                       | Masquerading (6)                         | Pre-OS Boot (5)                          | Pre-OS Boot (5)                         | Unsecured Credentials (4)               | Process Groups Discovery (3)           |                                           | Email Collection (3)                   | Proxy (4)                             |                                       |                               |
|                                        |                               |                                     | Scheduled Task/Job (4)                | Modify Authentication Process (4)        | Scheduled Task/Job (4)                   | Scheduled Task/Job (4)                  | Modify Cloud Compute Infrastructure (4) | Process Discovery                      |                                           | Input Capture (4)                      | Remote Access Software                |                                       |                               |
|                                        |                               |                                     | Server Software Component (2)         | Modify Registry                          | Server Software Component (2)            | Server Software Component (2)           | Modify Registry                         | Query Registry                         |                                           | Man in the Browser                     | Traffic Signaling (1)                 |                                       |                               |
|                                        |                               |                                     | Traffic Signaling (1)                 | Modify System Image (2)                  | Traffic Signaling (1)                    | Traffic Signaling (1)                   | Modify System Image (2)                 | Remote System Discovery                |                                           | Man-in-the-Middle (2)                  | Web Service (3)                       |                                       |                               |
|                                        |                               |                                     | Valid Accounts (4)                    | Network Boundary Bridging (1)            | Valid Accounts (4)                       | Valid Accounts (4)                      | Network Boundary Bridging (1)           | Software Discovery (1)                 |                                           | Screen Capture                         |                                       |                                       |                               |
|                                        |                               |                                     |                                       | Obfuscated Files or Information (5)      |                                          |                                         | Obfuscated Files or Information (5)     | System Information Discovery           |                                           | Video Capture                          |                                       |                                       |                               |
|                                        |                               |                                     |                                       | Pre-OS Boot (3)                          |                                          |                                         | Pre-OS Boot (3)                         | System Network Configuration Discovery |                                           |                                        |                                       |                                       |                               |
|                                        |                               |                                     |                                       | Process Injection (11)                   |                                          |                                         | Process Injection (11)                  | System Network Connections Discovery   |                                           |                                        |                                       |                                       |                               |
|                                        |                               |                                     |                                       | Rogue Domain Controller Rootkit          |                                          |                                         | Rogue Domain Controller Rootkit         | System Owner/User Discovery            |                                           |                                        |                                       |                                       |                               |
|                                        |                               |                                     |                                       | Signed Binary Proxy Execution (11)       |                                          |                                         | Signed Binary Proxy Execution (11)      | System Service Discovery               |                                           |                                        |                                       |                                       |                               |
|                                        |                               |                                     |                                       | Signed Script Proxy Execution (1)        |                                          |                                         | Signed Script Proxy Execution (1)       | System Time Discovery                  |                                           |                                        |                                       |                                       |                               |
|                                        |                               |                                     |                                       | Subvert Trust Controls (4)               |                                          |                                         | Subvert Trust Controls (4)              | Virtualization/Sandbox Evasion (3)     |                                           |                                        |                                       |                                       |                               |

**Enterprise**

14 тактик  
185 техник  
367 суб-техник  
Бесчётное число процедур  
v9



# ФСТЭК в новой методике оценки угроз стала использовать схожую концепцию

Только процедуры назвав сценариями реализации угроз



# Методика оценки угроз безопасности информации

Утверждена 5 февраля 2021 года

ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России  
5 февраля 2021 г.

**МЕТОДИЧЕСКИЙ ДОКУМЕНТ**  
**МЕТОДИКА**  
**ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ**

# Вся новая методика ФСТЭК на одном слайде

- Берем все угрозы и исключаем те, которые
  - Не приводят к негативным последствиям (ущербу)
  - Не связаны с нарушителями нужного типа с нужными ему целями
  - Направлены на активы, которых у вас отсутствуют
  - Требуют от нарушителей доступа, которого у них нет
- Для оставшихся угроз
  - Определите хотя бы один сценарий реализации угроз (10 тактик и 145 техник или MITRE ATT&CK с 200+ техниками)
  - Ранжируйте угрозы

**Это если применить здравый смысл и пообщаться с регулятором,  
а не читать текст буквально!**

# Этапы оценки угроз

Не совсем корректная  
последовательность, но это не  
так уж и важно

1. **Определение негативных последствий**
2. Инвентаризация систем и сетей
3. Определение источников угроз
4. Оценка способов реализации угроз
5. Оценка возможности реализации угроз и определение их актуальности
6. Оценка сценариев реализации угроз

# Что надо систематизировать?

Много неочевидных шагов, которые на последнем этапе не учитываются, так как техники высокоуровневые и не учитывают объект воздействия

- ❑ 8 типов объектов воздействия x 6 видов воздействия x 5 уровней воздействия = 240 элементов x # объектов
- ❑ Виды нарушителей
- ❑ Виды возможностей нарушителей
- ❑ Категории нарушителей
- ❑ Основные способы реализации угроз
- ❑ Интерфейсы воздействия
- ❑ Сценарии угроз
- ❑ Актуальные угрозы

# ФСТЭК в 1-м квартале 2022 года планирует внесение изменений в методику оценки



Новый БДУ, устранение нестыковок и лишних шагов,  
изменение процедуры оценки актуальности угроз, изменение  
подхода к сценариям реализации угроз

## От общего к частному

- ❑ Следуя методике, берем все возможные угрозы
- ❑ Отсекаем лишнее
- ❑ Оставляем только актуальные угрозы

## От частного к общему

- ❑ Берем реальные инциденты на значимых объектах КИИ и АСУ ТП
- ❑ Описываем эти сценарии реализации угроз
- ❑ Добавляем еще потенциально возможные

## Давайте все-таки вспомним про Stuxnet

Хотя в приличном обществе его уже  
и не вспоминают



- ❑ Считается первым примером проявления воздействия кибератак на физический мир (это не так)
- ❑ Две версии произошедшего – вредонос на флешке (самая популярная) и supply chain



# Stuxnet на одном слайде (согласно популярной версии)

Матрица MITRE ATT&CK позволяет описать все техники, используемые вредоносным кодом Stuxnet

- T1050
- T1120
- T1078
- T1109
- T1012
- T1091
- T1116
- T1058
- T1077
- T1055
- T1087
- T1105
- T1093
- T1063
- T1016
- T1014
- T1135
- T1082
- T1036
- T1046
- T1043
- T1107
- T1053
- T1092
- T1027
- T1106
- T1024
- T1134
- T1047
- T1132
- T1068
- T1068

# Почему MITRE ATT&CK?

MITRE ATT&CK является самым признанным и популярным подходом к описанию техник злоумышленников

- ❑ Понимание источников телеметрии для обнаружения
- ❑ Формирование тестов для Red Team / пентестов
- ❑ Выбор и тестирование средств защиты
- ❑ Понимание хакерских группировок (нарушителей), использующих эти техники
- ❑ Маппирование вредоносных программ в конкретные техники и тактики

# BlackEnergy на одном слайде

Матрица MITRE ATT&CK  
позволяет описать все техники,  
используемые в BlackEnergy

- T1548.002
- T1574.010
- T1113
- T1071.001
- T1070
- TT1553.006
- T1547.001
- T1070.001
- T1082
- T1547.009
- T1056.001
- T1016
- T1543.003
- T1046
- T1049
- T1555.003
- T1120
- T1552.001
- T1485
- T1057
- T1047
- T1008
- T1055.001
- T1083
- T1021.002

## Winnti Group на одном слайде

Китайская группировка, которая атаковала в том числе и российские промышленные предприятия в 2020-м году

- T1057
- T1543.003
- T1057
- T1014
- T1140
- T1055.001
- T1553.002
- T1573.001
- T1129
- T1543.003
- T1008
- T1518.001
- T1036.005
- T1105
- T1553.002
- T1218.011
- T1036.005
- T1082
- T1548.002
- T1112
- T1016
- T1134.002
- T1106
- T1124
- T1134.004
- T1095
- T1547.012
- T1027

А еще можно использовать  
специализированную матрицу  
ATT&CK for ICS



# HAVEX на одном слайде. Он же Backdoor.Oldrea

Это одна из специализированных для АСУ ТП вредоносных программ

## ICS

- ❑ T850
- ❑ T808
- ❑ T846
- ❑ T825
- ❑ T814
- ❑ T862
- ❑ T865
- ❑ T802
- ❑ T863
- ❑ T861

## Enterprise

- ❑ T1003
- ❑ T1022
- ❑ T1001
- ❑ T1114
- ❑ T1083
- ❑ T1107
- ❑ T1057
- ❑ T1055
- ❑ T1060
- ❑ T1082
- ❑ T1016
- ❑ T1033
- ❑ T1070.004
- ❑ T1132.001
- ❑ T1555.003
- ❑ T1547.001
- ❑ T1560
- ❑ T1087

## Достаточно ли нам этого?

Вообще да, но так нет



- ❑ В России есть свои требования по описанию тактик и техник атак
- ❑ Тактики и техники угроз из методики оценки угроз ФСТЭК не маппируются в TTP MITRE ATT&CK
- ❑ Несмотря на то, что все распространенные на российском рынке средства защиты используют именно TTP от MITRE ATT&CK

# А можем мы смаппить TTP от MITRE ATT&CK в тактики и техники ФСТЭК?



Было бы неплохо, если бы это сделала сама ФСТЭК, но пока увы... Хотя есть другие варианты





## Угроза для Чернобыльской АЭС

Вредоносный код Netya, который  
многие называют NotPetya

- ❑ Попадание вредоносного кода в систему мониторинга радиационного фона
- ❑ Переход на ручной мониторинг
- ❑ Неработоспособность системы электронного документооборота
- ❑ Неработоспособность сайта АЭС

## Netya на одном слайде

Матрица MITRE ATT&CK позволяет описать все техники, используемые в инциденте на Чернобыльскую АЭС

- T1486
- T1210
- T1083
- T1070.001
- T1036
- T1003.001
- T1021.002
- T1053.005
- T1218.011
- T1518.001
- T1569.002
- T1529
- T1078.003
- T1047

# Соответствие техник MITRE ATT&CK и ФСТЭК

|                                                               |                                                                                                                                                                                             |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T1486 Data Encrypted for Impact                               | Отсутствует                                                                                                                                                                                 |
| T1210 Exploitation of Remote Services                         | T8.1 Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа                                           |
| T1083 File and Directory Discovery                            | T1.9 Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО       |
| T1070.001 Indicator Removal on Host: Clear Windows Event Logs | T7.2. Очистка/затирание истории команд и журналов регистрации                                                                                                                               |
| T1036 Masquerading                                            | Отсутствует                                                                                                                                                                                 |
| T1003.001 OS Credential Dumping: LSASS Memory                 | T1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа) |

# Соответствие техник MITRE ATT&CK и ФСТЭК

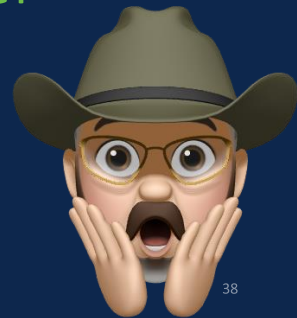
|                                                           |                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T1021.002 Remote Services: SMB/Windows Admin Shares       | T8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям                                                                                                                                                                        |
| T1053.005 Scheduled Task/Job: Scheduled Task              | T3.15. Планирование запуска вредоносных программ через планировщиков задач в операционной системе<br>T4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети |
| T1218.011 Signed Binary Proxy Execution: Rundll32         | Отсутствует                                                                                                                                                                                                                                                                             |
| T1518.001 Software Discovery: Security Software Discovery | Отсутствует в явной форме, только косвенно – T1                                                                                                                                                                                                                                         |
| T1569.002 System Services: Service Execution              | T3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных                                                                                                                                                      |
| T1529 System Shutdown/Reboot                              | T10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети<br>T10.12. Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления                                          |

# Соответствие техник MITRE ATT&CK и ФСТЭК

|                                          |                                                                                                                                                                                               |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T1078.003 Valid Accounts: Local Accounts | T2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации<br>T4.1. Несанкционированное создание учетных записей или кража существующих учетных данных и др. |
| T1047 Windows Management Instrumentation | Отсутствует                                                                                                                                                                                   |

# К сожалению прямой маппинг всех техник и тактик ФСТЭК в ТТР MITRE ATT&CK невозможен

ФСТЭК не имеет ряда техник (145 vs 200+), а также не имеет детализации для конкретных платформ – Windows, Linux, мобильных устройств, облачных платформ и т.п.



# Угроза для БелАЭС\*

Апрель 2021

- ❑ Взлом сайта и размещение объявления об опасности объекта

\* - Белорусская АЭС, не путать с Белярской АЭС

# Подмена главной страницы сайта

Всего одна угроза, но имеющая  
серьезные последствия

- T10.9 Добавление информации



## Шифровальщики

Многие предприятия из сферы промышленности, ТЭК и т.п. сталкиваются с шифровальщиками, которые хотя и не проникают в АСУ ТП, но приводят к останову бизнес-операций и реализации негативных последствий



Colonial Pipeline Company



## 2019-й год

- ❑ T1564.003 – Hidden Window
- ❑ T1497 – Virtualization / Sandbox Evasion
- ❑ T1547.001 – Registry Run Keys / Startup Folders
- ❑ T1490 – Inhibit System Recovery
- ❑ T1112 – Modify Registry
- ❑ T1542.003 - Bootkit
- ❑ T1057 – Process Discovery
- ❑ T1036 - Masquerading
- ❑ T1564.001 – Hidden Files & Directories
- ❑ T1016 – System Network Configuration Discovery

## 2020-й год

- ❑ T1133 - External Remote Services
- ❑ T1059 - Command & Scripting Interpreter
- ❑ T1053 - Scheduled Task
- ❑ T1078 - Valid Accounts
- ❑ T1055 - Process Injection
- ❑ T1110 - Brute Force
- ❑ T1003 - OS Credential Dumping
- ❑ T1018 - Remote System Discovery
- ❑ T1021 - Remote Services
- ❑ T1486 - Data Encrypted for Impact

# Соответствие техник MITRE ATT&CK и ФСТЭК

|                                         |                                                                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| T1133 - External Remote Services        | T2.1 – Использование внешних сервисов                                                                                              |
| T1059 - Command & Scripting Interpreter | T3.1 – Автоматический запуск скриптов и исполняемых файлов                                                                         |
| T1053 - Scheduled Task/Job              | T3.14/T3.15 – Планирование запуска вредоносных программ при старте ОС/через планировщики                                           |
| T1078 - Valid Accounts                  | T2.11 – Несанкционированный доступ путем компрометации учетных данных сотрудника организации                                       |
| T1055 - Process Injection               | T7.10 - Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты                                    |
| T1110 - Brute Force                     | T2.10 - Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя                            |
| T1003 - OS Credential Dumping           | T1.9 - Сбор информации..., включая поиск паролей в исходном и хэшированном виде, криптографических ключей                          |
| T1018 - Remote System Discovery         | Отсутствует (наиболее близко T1.3 – Пассивный сбор / прослушивание/ и T1.4 – Направленное сканирование при помощи специального ПО) |
| T1021 - Remote Services                 | T8.2 - Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям                  |
| T1486 - Data Encrypted for Impact       | Отсутствует                                                                                                                        |

Обратите внимание, что при триллионах комбинаций сценариев реализации угроз число техник у вас все равно ограничено парой-тройкой сотен



Так может ориентироваться на техники, а не их комбинации?  
А техники брать не из головы, а из известных инцидентов?



# Перевод всех техник MITRE ATT&CK Enterprise v9 на русский язык

ATT&CK for ICS на подходе



| ID                    | Название                                                                           | Исходный вариант                  |
|-----------------------|------------------------------------------------------------------------------------|-----------------------------------|
| <a href="#">T1548</a> | Злоупотребление механизмом контроля повышения привилегий                           | Abuse Elevation Control Mechanism |
|                       | .001 Использование битов Setuid и Setgid                                           | Setuid and Setgid                 |
|                       | .002 Обход контроля учетных записей пользователей                                  | Bypass User Account Control       |
|                       | .003 Выполнение команд от имени другого пользователя через Sudo и кеширование Sudo | Sudo and Sudo Caching             |
|                       | .004 Повышение привилегий через запрос учетных данных                              | Elevated Execution with Prompt    |
| <a href="#">T1134</a> | Манипуляции с токенами доступа                                                     | Access Token Manipulation         |
|                       | .001 Подмена/кража токена                                                          | Token Impersonation/Theft         |
|                       | .002 Создание процессов с помощью токенов                                          | Create Process with Token         |
|                       | .003 Создание и подмена токена                                                     | Make and Impersonate Token        |
|                       | .004 Подмена родительского PID                                                     | Parent PID Spoofing               |
|                       | .005 Инъекция SID-истории                                                          | SID-History Injection             |
| <a href="#">T1531</a> | Блокировка доступа к учетной записи                                                | Account Access Removal            |
| <a href="#">T1087</a> | Поиск учетных записей                                                              | Account Discovery                 |
|                       | .001 Поиск локальной учетной записи                                                | Local Account                     |

<https://t.me/alukatsky>

# Маппинг всех техник методики оценки угроз ФСТЭК в MITRE ATT&CK Enterprise v9

## ATT&CK for ICS на подходе



| Сбор информации - T1 |                                                                                                                                                                                                                                                                                                                                                  |                                  |             |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|-------------|
| ID TTY               | Название техники                                                                                                                                                                                                                                                                                                                                 | ID MITRE ATT&CK                  | Комментарий |
| T1.1                 | Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций                                                                                                                                                                              | T1593<br>T1594<br>T1596<br>T1591 |             |
| T1.2                 | Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.                                                                                                           | T1593                            |             |
| T1.3                 | Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей                                                                                                                                 | T1589<br>T1592<br>T1590          |             |
| T1.4                 | Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. | T1595<br>T1592<br>T1590          |             |
| T1.5                 | Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств.                                                                                            | T1595<br>T1590<br>T1589<br>T1592 |             |

<https://t.me/alukatsky>

# ФСТЭК планирует разработать маппинг техник и тактик угроз в защитные меры

Не ранее 2022 года



# В качестве заключения

- Моделирование угроз – важная составляющая процесса ИБ АСУ ТП
- В конце 2021-го – начале 2022-го года методика ФСТЭК будет изменяться
- Начинать оценку угроз проще не с перебора всех возможных сценариев, а с анализа реальных инцидентов и используемых в них тактик и техник
- За основу можно взять MITRE ATT&CK и ее маппинг на техники ФСТЭК





# Дополнительная информация

- <https://attack.mitre.org/> - проект MITRE ATT&CK
- [https://collaborate.mitre.org/attackics/index.php/Main\\_Page](https://collaborate.mitre.org/attackics/index.php/Main_Page) - проект MITRE ATT&CK for ICS
- <https://www.fstec.ru/> - сайт ФСТЭК России
- <https://bdu.fstec.ru/> - Банк данных угроз и уязвимостей ФСТЭК
- <https://t.me/alukatsky> - канал «Пост Лукацкого», где будут выложены перевод MITRE ATT&CK и маппинг техник ФСТЭК в MITRE ATT&CK
- <https://t.me/RuScadaSec> – канал «RUSCADASEC community: Кибербезопасность АСУ ТП»



SECURE