Lucrarea de laborator nr. 1

Analiza incidentelor de securitate informațională

Scop

Scopul lucrării este familiarizarea cu noțiunile de bază ale securității informaționale prin analiza unui incident real de securitate și evaluarea impactului acestuia asupra unui sistem informațional.

Cerință generală

Alegeți **un incident real de securitate informațională**, produs în ultimii **10 ani**, și realizați o analiză structurată a acestuia, conform cerințelor de mai jos.

Incidentul trebuie documentat din **surse publice credibile** (rapoarte oficiale, articole tehnice, comunicate ale organizațiilor afectate).

Cerințe obligatorii

1. Descrierea incidentului

Prezentați succint incidentul ales, indicând:

- organizația sau instituția afectată;
- anul producerii incidentului;
- tipul incidentului (ex.: breșă de date, ransomware, APT, compromitere de conturi);
- vectorul principal de atac (dacă este cunoscut).

2. Identificarea activelor afectate

Identificați și descrieți:

- tipurile de date compromise;
- sistemele sau serviciile afectate;
- categoriile de utilizatori impactați.

3. Analiza impactului (Triada CID)

Analizați impactul incidentului asupra:

- **Confidențialității**;
- **Integrității**;
- **Disponibilității**.

Pentru fiecare componentă, explicați dacă și cum a fost afectată.

4. Cauze și vulnerabilități

Indicați:

- vulnerabilități tehnice sau organizaționale exploatate;
- erori de configurare sau lipsa unor controale de securitate;
- rolul factorului uman (dacă este cazul).

5. Măsuri de prevenire

Propuneți **minimum 5 măsuri concrete** care ar fi putut preveni sau reduce impactul incidentului, raportate la bune practici de securitate informațională.

Лабораторная работа №1

Анализ инцидентов информационной безопасности

Цель работы

Целью данной лабораторной работы является ознакомление с основными понятиями информационной безопасности посредством анализа реального инцидента безопасности и оценки его влияния на информационную систему.

Общее требование

Выберите **реальный инцидент информационной безопасности**, произошедший за последние **10 лет**, и выполните его структурированный анализ в соответствии с требованиями, приведёнными ниже.

Инцидент должен быть описан на основе **достоверных публичных источников** (официальные отчёты, технические статьи, заявления пострадавших организаций).

Обязательные требования

1. Описание инцидента

Кратко опишите выбранный инцидент, указав:

- организацию или учреждение, пострадавшее в результате инцидента;
- год возникновения инцидента;
- тип инцидента (утечка данных, ransomware, APT, компрометация учётных записей);
- основной вектор атаки (если известен).

2. Определение затронутых активов

- Определите и опишите:
- типы скомпрометированных данных;
- затронутые системы или сервисы;
- категории пользователей, подвергшиеся воздействию инцидента.

3. Анализ воздействия (триада CID)

Проанализируйте влияние инцидента на:

- **Конфиденциальность**;
- **Целостность**;
- **Доступность**.

Для каждого элемента укажите, был ли он нарушен и каким образом.

4. Причины и уязвимости

Укажите:

- технические или организационные уязвимости, которые были использованы;
- ошибки конфигурации или отсутствие необходимых мер безопасности;
- роль человеческого фактора (при наличии).

5. Меры предотвращения

Предложите **не менее 5 конкретных мер**, которые могли бы предотвратить инцидент или снизить его последствия, опираясь на лучшие практики информационной безопасности