Алгоритм Розслідування та експертизи кіберінцидентів/ кібератак

CyberLab
Комп'ютерна криміналістика

Мета

Підтвердження факту втручання сторонніх осіб в роботу інформаційно-телекомунікаційної системи підприємства, яке призвело до спотворення та зупинки процесу обробки інформації

Цілі:

- Фіксація та збереження цифрових доказів, документальне оформлення процесу
- Аналіз цифрових доказів для встановлення обставин та обсягу кіберінциденту
- Відновлення даних та процесів (враховуючи наслідки кіберінциденту)
- Підготовка відповідних документів (звітів, висновків судової експертизи, довідок, тощо) для передачі до правоохоронних органів

ЮРИДИЧНА СКЛАДОВА
Для досягнення мети укладається ДОГОВІР про надання послуг.
Супутньо укладається договір про нерозголошення комерційної та конфіденційної інформації

CyberLab
Комп'ютерна криміналістика

далі

Процеси

Підготовчий етап

Погодження юридичних аспектів взаємодії сторін та підписання відповідних договрів

Попередній етап

Проведення зустрічі, під час якої створюється робоча група та визначаються механізми взаємодії, враховуючи комунікацію між виконавцями та представниками та технічну складову проведення розслідування

CyberLab
Комп'ютерна криміналістика

далі

ЕТАПИ ВИКОНАННЯ

Пошук, фіксація та збір цифрових доказів

– Проведення внутрішнього опитування (інтерв'ю) персоналу, що має причетність до роботи інформаційно–телекомунікаційної системи
– Створення копій носіїв інформації з обладнання, що зазнали втручання
– Документальне оформлення процедур створення

Попередній аналіз зібраних цифрових доказів

– Аналіз зібраної інформації, (пошук по критеріям)
– Реконструкція схеми та хронології кіберінциденту та встановлення його обсягу і наслідків
– Підготовка відповідних документів (звітів, висновків судової експертизи, довідок, тощо) для передачі до правоохоронних органів (за потреби)

CyberLab
Комп'ютерна криміналістика

Відновлення даних та процесів

Відновлення даних:
- відновлення інформації з резервних копій;
перевірка цілісності даних (щоб переконатися, що копії не пошкоджені чи не скомпрометовані);
-синхронізація відновлених даних з актуальними.

Відновлення систем і сервісів:
- пуск або перевстановлення з «чистих» образів
- застосування оновлень та патчів;
- повторна перевірка безпеки (сканування на віруси, уразливості).