УДК 007.2 **Ткаченко І.В., Козачок В.А., Гахов С.О., Дмітрієв В.Є.**
DOI: 10.31673/2409-7292.2020.015457

ОЦІНКА СТАНУ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В ХОДІ ВИЯВЛЕННЯ ТА ВІДСЛІДКОВУВАННЯ КРИЗОВИХ ІНДИКАТОРІВ

В статті розглянуто питання щодо оцінки стану кібербезпеки об'єктів критичної інформаційної інфраструктури з урахуванням індикаторів кіберзагроз будь якого масштабу та пошук кореляції між: даними аудиту стану захищеності об'єктів критичної інфраструктури, даних щодо оцінки ризиків та моделей кіберзагроз, данні про індикатори, що передують відомим кіберзагрозам.

Ключові слова: інформаційна система, оцінка стану, кібербезпека, критична інформаційна інфраструктура, індикатори кіберзагроз, машинне навчання, великі дані.

Вступ

В умовах сьогодення України актуальним є питанням формування системи управління кібербезпекою критичної інформаційної інфраструктури основним завданням якої є раннє виявлення та відслідковування кризових індикаторів, що передують та/або є характерними для тієї чи іншої кіберзагрози.

При вивчені історичних процесів виявлено, що до початку втілення кіберзагрози у спрямовані кібератаки чи інші види кіберзлочинності призводить ряд факторів, які збігаються в певний момент часу та можуть класифікуватись за сукупністю загроз як кризова точка(точка біфуркації).[1] Також слід враховувати, що кібератаки мають різні фази, частоту повторень, періоди та види, тому встановлення поняття кризової точки важливе для вірної поточної оцінки стану кібербезпеки об'єктів критичної інфраструктури.

Суб'єкти забезпечення кібербезпеки мають визначати поняття кризової точки згідно затверджених шаблонів та в процесі оцінки стану кіберзахисту збагачувати шаблони кризишляхом оновлення(уточнення) індексів. Кожен індекс має певне кількісне та якісне значення, яке розраховується шляхом об'єднання значень декількох математичних розрахункових показників. [2]

З метою розуміння підходу до визначення кризових точок необхідно врахувати:

-міжнародні та регіональні індекси щодо оцінки кіберризиків; - порядок та етапи організації оцінки стану кібербезпеки, з урахуванням відомих індикаторів кіберзагроз; - технологія великих даних як основний інструмент здійснення заходів з оцінки та відслідковування в режимі реального часу стану кібербезпеки об'єктів критичної інфраструктури. Існують визначені міжнародні, загальнодержавні та регіональні індекси щодо оцінки, аналізу, класифікації кіберзагроз та оцінки ризиків, що вони несуть, а також індекси оцінки готовності ІТ інфраструктур держав (організацій) до боротьби з кібератаками (рис. 1).[3][4]

Також існують типові моделі кіберзагроз та методи класифікації кібератак з використанням різноманітних типів експертних систем. В ході класифікацій та аналізу атаки використовуються державні, комерційні та не комерційні центри обміну інформацією про кіберінциденти, та індикатори кіберзагроз, що їм передують, з занесенням структурованої інформації про кіберінцидент до єдиного реєстру.[5] Це дозволяє проводити аналіз кіберінцидентів та виявляти певні закономірності(індикатори кіберзагроз), які складаються з показників щодо ступеня небезпеки того чи іншого виду кібератаки (у разі класифікації), векторної направленості кіберзагрози, сукупність методів, що були застосовані при кібератаці, критичності збитку при вжитті захисних заходів в той чи інший момент часу.[6]

Оцінка стану кібербезпеки об'єктів критичної інформаційної інфраструктури з урахуванням індикаторів кіберзагроз будь якого масштабу є об'єднанням та пошуком кореляції між:

- даними аудиту стану захищеності об'єктів критичної інфраструктури;

- даних щодо оцінки ризиків та моделей кіберзагроз;
- даними про індикатори, що передують відомим кіберзагрозам.

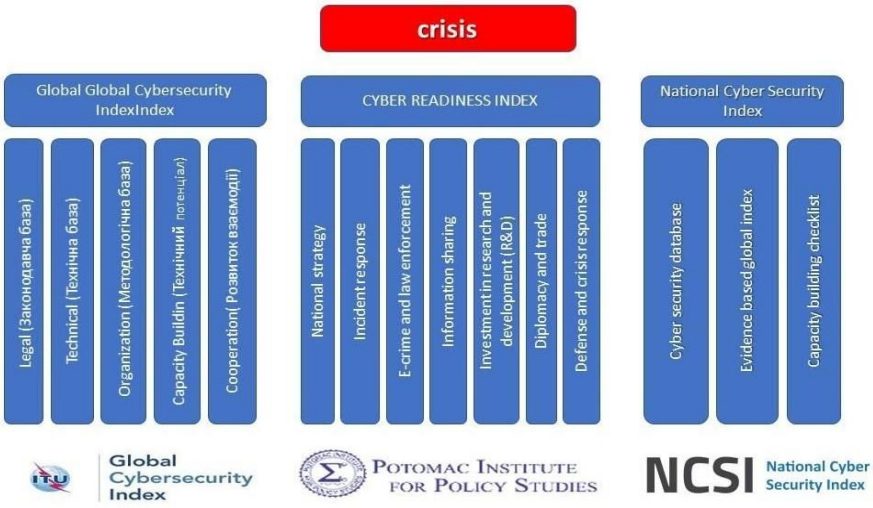

Рис. 1. Індекси оцінки готовності ІТ інфраструктур держав (організацій) до боротьби з кібератаками

Вищезазначена оцінка потребує використання датасету (набору даних), моделі та програмних засобів, що здійснять обробку датасету за зазначеною моделлю, що дозволить визначити стан кібербезпеки об'єктів критичної інфраструктури на поточний момент часу, та\або його відхилення за певними індикаторами.

Ключовим моментом є вибір типів даних та джерел інформації, на основі яких буде здійснюватися оцінка. Слід вказати, що всі можливі вхідні дані, з яких буде сформовано датасет розподіляються на структуровані та не структуровані.

Якість оцінки буде залежати від наступних факторів:

- визначення основного переліку індексів щодо оцінки кібербезпеки типових для даного об'єкту критичної інфраструктури;
- здійснення збагачення(уточнення) даних моделі шляхом введення регіональних індексів;
- застосування технології великих даних для роботи з структурованими та не структурованими даними;
- вибору технології машинного навчання, що буде здійснювати обробку даних моделі, її тренування та перенавчання;
- здійснення кореляції та виявлення залежностей між індексами (створення шаблону індикаторів);
- визначення дельти часу (вікна спостереження), період за який буде здійснено спостереження. [7]

В ході оцінки може знадобитись проведення очистки даних та таргетування датасету, для цього можливо слід задіяти експертну систему чи визначити певну роль експерта з даних, що зможе визначити взаємопов'язані ключові індикатори. [8]

Окремими питання стоїть доставка даних про стан ІТ інфраструктури об'єкту критичної інфраструктури в режимі реального часу та порівняння цих даних з даними моделі для пошуку відхилень, та виявлення початку зміни параметрів індикаторів, що призведуть до появи певного індексу, що в свою чергу дозволить виявляти кіберзагрозу на ранній стадії. Також слід відокремити питання прогнозування результатів виникнення кіберзагроз з

врахуванням вищезазначеної оцінки, та впливу цих результатів на стан кібербезпеки об’єкту критичної інфраструктури. Модель прогнозування повинна використовувати дані оцінки, проте базуватись на інших математичних інструментах. На основі отриманого результату здійснюються подальшої побудови сценаріїв розвитку кібератак, що дозволить їх використовувати в інших експертних системах.[9]

На оцінку впливає стан пов’язаних з об’єктом критичної інфраструктури взаємодіючих систем. На сьогоднішній день відбувається загальне об’єднання IT інфраструктури (діджиталізація), тому оцінка стану одного об’єкту критичної інфраструктури впливає на інший, пов'язаний з ним.

Щодо технічних аспектів технологія машинного навчання та роботи з великими даними слід дотримуватись Cross-industry standard process for data mining (рис 2).[10]

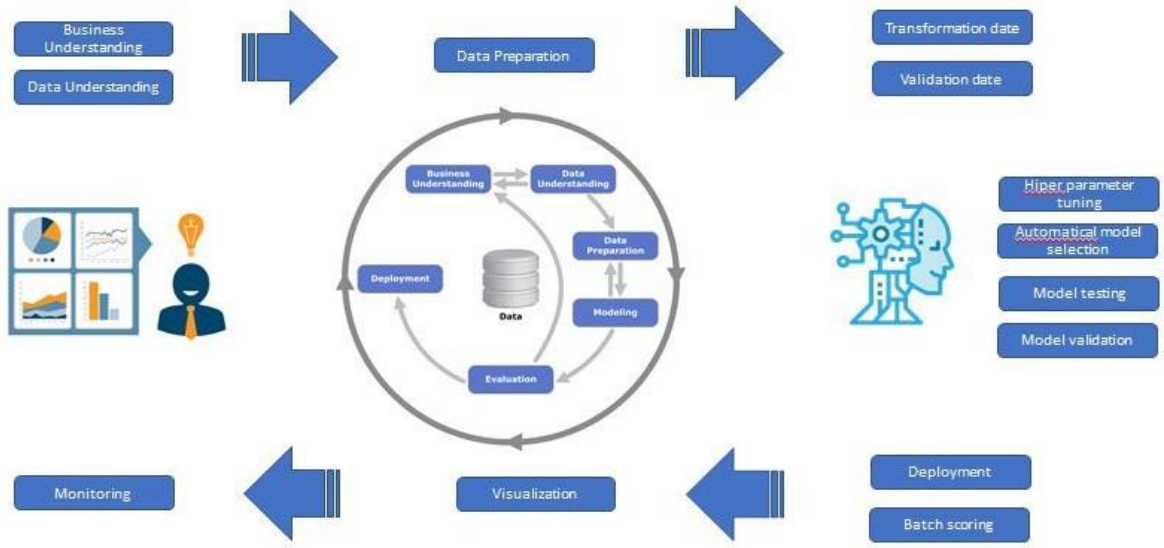

Рис 2. Cross-industry standard process for data mining

В хорді навчання моделі потрібно визначити шаблон індикаторів кіберзагроз, відповідно за якими необхідно здійснювати заходи моніторингу, або шукати додаткові джерела для отримання показників за ними. Для класифікації даних слід використовувати алгоритми на кшталт Random Forest, точність якого залежить від кількості даних. Використання машинного навчання надасть можливість провести ряд експериментів з наборами даних та провести навчання моделей. В ході роботи буде здійснено кореляцію та виявлення залежностей між індексами. Підготовку, обробку та візуалізацію даних можливо виконувати у стеці технологій подібних до платформ хмарного обчислення, що передбачає високу відмовостійкість та масштабованість.

Висновок

Висновки оцінки стану спроможності кіберзахисту IT інфраструктури об'єкту критичної інформаційної інфраструктури, щодо виявлення, попередження інцидентів кібербезпеки повинні відповідати міжнародним стандартам (ISO 2700x, NIST, AICPA, HITRUST, COBIT, PCI DSS, GDPR, SOX, SWIFT, HIPPA, NYDFS).

Впровадження оцінки стану кібербезпеки об’єктів критичної інформаційної інфраструктури в режимі реального часу, з використання індикаторів кіберзагроз на рівні прийняття рішень дозволить забезпечити інформацією загальнодержавний центр кіберстікості CRC (Cyber Resilience Center) у разі його створення.

Перелік посилань

1. https://en.wikipedia.org/wiki/Catastrophe_theory (05.04.2020)
2. Itu.int [Електронний ресурс] // - Режим доступу: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
3. Marsh.com [Електронний ресурс] // - Режим доступу:https://www.marsh.com/ru/ru/insights/research-briefings/marsh-microsoft-cyber-survey-report-2019.html
4. First.org [Електронний ресурс] // - Режим доступу:https://www.first.org/cvss/
5. Закон України «Про основні засади забезпечення кібербезпеки України».
6. Олександр Корченко, Віктор Гнатюк, Євгенія Іванченко, Сергій Гнатюк, Нургуль Сейлова. Метод мережево-центричного моніторингу кіберінцидентів в сучасних інформаційно-телекомунікаційних системах. Захист інформації, Том 18, №3, липень-вересень 2016.
7. Гаськова Д.А.1, Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры. DOI 10.21681/2311-3456-2019-2-42-49
8. Jason W. Osborne. Best Practices in Data Cleaning: A Complete Guide to Everything You Need to Do Before and After Collecting Your Data . - Sage, 2012. - 275p.
9. https://en.wikipedia.org/wiki/Cyber_threat_hunting
10. https://ru.wikipedia.org/wiki/CRISP-DM
11. https://en.wikipedia.org/wiki/cyber_resilience_review.

Надійшла: 19.01.2020 Рецензент: д.т.н., професор Вишнівський В.В.