УДК 338.242(477)

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЛОГІЧНИХ МОДЕЛЕЙ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Володимир Шиповський
Національний університет оборони України імені Івана Черняховського, v.shypovskyi@nuou.org.ua

Останні події в Україні, зокрема окупація Криму та широкомасштабне вторгнення росії, демонструють важливість забезпечення кібербезпеки об'єктів критичної інфраструктури. Російська Федерація використовує різні методи, включаючи ракетні та кібератаки, для здійснення впливу на інфраструктуру нащої країни та забезпечення своїх військових та політичних інтересів. Ці напади зумовлюють необхідність розвитку та застосування ефективних методів оцінювання кібербезпеки, щоб захистити інфраструктуру від можливих загроз та підвищити рівень безпеки. У даній статті будуть проаналізовані та порівняні різні логічні моделі оцінювання кібербезпеки інформаційних систем, які можуть бути застосовані для захисту об'єктів критичної інфраструктури в Україні.

Метою даної роботи є порівняльний аналіз логічних моделй оцінювання кіберстійкості інформаційних систем, а саме: DREAD, STRIDE, PASTA та CVSS, переваг та недоліків, та вибір оптимальної для загроз та ризиків об'єктів критичної інфраструктури.

Розлянемо найпоширеніші логічні моделі оцінювання кіберстійкості інформаційних систем, деякі з них наведені нижче:

1. Модель дерева загроз: ця модель використовує дерево загроз для оцінювання ризику кібератаки. Кожен вузол у дереві відповідає певній загрозі, а дуги показують ймовірність того, що ця загроза стане реальністю. З цієї моделі можна отримати інформацію про рівень загроз, а також про те, які частини інформаційної системи найбільш вразливі до атак.

2. Модель DREAD: ця модель використовує п'ять факторів для оцінювання ризику кібератаки: Damage, Reproducibility, Exploitability, Affected users та Discoverability. Кожен фактор оцінюється від 0 до 10, і загальний ризик визначається шляхом підрахунку середнього значення.

3. Модель STRIDE: ця модель використовує шість факторів для оцінювання ризику кібератаки: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, та Elevation of privilege. Кожен фактор оцінюється від 0 до 10, і загальний ризик визначається шляхом підрахунку середнього значення.

4. Модель CVSS: ця модель використовує 3 метрики для оцінювання ризику кібератаки: базова метрика, темпоральна метрика, та середовищна метрика. Базова метрика визначає ризик, який може виникнути при використанні вразливості, темпоральна метрика визначає, як швидко вразливість може бути виправлена, а середовищна метрика визначає, як вразливість впливає на систему в цілому.

Порівняльний аналіз моделей за основними характеристиками наведено у таблиці 1.

Таблиця 1

Порівняння характеристик моделей оцінювання

Характеристика	**Модель DREAD**	**Модель STRIDE**	**Модель CVSS**	**Модель дерева загроз**
Ступінь охоплення	Середній	Високий	Високий	Високий
Точність оцінювання	Висока	Середня/Висока	Висока	Середня/Висока
Швидкість оцінювання	Швидка	Помірна/Повільна	Повільна	Швидка
Розширюваність	Середня	Висока	Низька/Середня	Висока
Придатність до довгострокового використання	Висока	Висока	Висока	Висока
Частота виявлення нових загроз	Низька	Середня/Висока	Низька/Середня	Висока
Вартість розробки та підтримки	Середня	Середня/Висока	Висока/Дуже висока	Середня
Кількість помилок	Середня	Низька/Середня	Середня	Середня
Складність розробки та використання	Низька	Середня	Висока	Середня/Висока

Вибір оптимальної моделі для оцінювання кібербезпеки інформаційних систем саме об'єктів критичної інфраструктури залежить від конкретних потреб та обставин кожної організації. Однак, з урахуванням результатів порівняння чотирьох найбільш популярних моделей (DREAD, STRIDE, Attack Tree та CVSS), можна зробити висновок, що найбільш оптимальним варіантом буде модель CVSS.

Модель CVSS є стандартом, розробленим групою спеціалістів з кібербезпеки та затвердженим міжнародною організацією FIRST. Ця модель оцінює рівень вразливості і потенційну шкоду, що може бути завдана, враховуючи широкий спектр факторів. Крім того, CVSS надає різні метрики, такі як базовий рівень вразливості, вплив та відсутність відповіді на вразливість, що дозволяє оцінювати кібербезпеку з точністю та деталізацією.

Додатково, модель CVSS відрізняється від інших моделей тим, що враховує контекст індивідуального застосування. Це означає, що оцінка кібербезпеки буде більш точною та зрозумілою, оскільки враховується конкретне застосування інформаційної системи.

Отже, модель CVSS є оптимальним варіантом для оцінювання кібербезпеки інформаційних систем об'єктів критичної інфраструктури через її точність, деталізацію та врахування контексту індивідуального застосування

Науковий керівник – д.т.н., проф. Микусь С.А.