Охрімчук В.В., к.т.н., професор,
Гуменюк І.В., к.т.н., доцент,
Охрімчук І.А., викладач
Житомирський військовий інститут імені С.П. Корольова

ПРОБЛЕМИ ВИЗНАЧАННЯ РІВНЯ КІБЕРЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Сьогодні питання кіберзахисту все більш актуалізується, оскільки відбувається стрімкий ріст кількості та технологічної складності кібератак та загроз кібербезпеці об'єктів критичної інформаційної інфраструктури [1]. В цьому контексті рівень їх кіберзахищеності стає однією з ключових характеристик, оскільки визначає стійкість до кібератак та забезпечує захист важливої інформації від несанкціонованого доступу, втрати або пошкодження. Водночас, визначення рівня кіберзахищеності стає складною задачею, оскільки вимоги до безпеки залежать від різних факторів, таких як розмір об'єкту та його інформаційно-комунікаційних систем, тип діяльності, тип інформації, що зберігається та обробляється, інфраструктура, рівень кваліфікації персоналу тощо.

Для визначення рівня кіберзахищеності використовуються різні методики та стандарти, такі як *ISO/IEC* 27001, *NIST Cybersecurity Framework, CIS Controls* та інші. Ці методики надають комплексний підхід до визначення рівня кіберзахищеності та містять рекомендації та вказівки для зменшення ризиків та запобігання кіберзагрозам [2].

У процесі визначення рівня кіберзахищеності необхідно провести аналіз систем об'єкта критичної інформаційної інфраструктури та виявити потенційні кіберзагрози та ризики, які можуть вплинути на його функціонування.

Проте при визначенні рівня кіберзахищеності будь-якого об'єкту критичної інформаційної інфраструктури виникає ціла низка проблем, які можуть мати суттєвий вплив на адекватність отриманих результатів.

Перш за все, одна з основних проблем полягає в тому, що сьогодні відсутня загальна система оцінки та стандарти в галузі кібербезпеки [1]. На сьогодні існує багато різних підходів та методик оцінки рівня кіберзахищеності, але вони часто відрізняються між собою та не мають загального стандарту. Це може призвести до того, що використання різних методик та метрик оцінки кіберзахищеності ускладнює порівняння та аналіз рівня кібербезпеки між різними організаціями та компаніями.

Крім того, ще одна проблема полягає в тому, що кіберзахист є динамічним процесом, який постійно адаптується до нових загроз та викликів [3]. Тому визначений раніш рівень кіберзахищеності об'єкту критичної інформаційної структури може бути застарілий вже за кілька місяців та не відповідати реальному показнику.

Також важливо зазначити, що кіберзахист – це не тільки технічний аспект, але й людський. Наприклад, найсильніша парольна політика не буде ефективною, якщо користувачі не дотримуються її правил. Тому визначення рівня кіберзахищеності має включати в себе не тільки технічні аспекти, але і процеси управління ризиками та навчання користувачів.

Не слід ігнорувати і таку проблеми як неврахування сфери застосування та невірне визначення пріоритетів. Визначення рівня кіберзахищеності повинна проводитись з урахуванням сфери застосування. Наприклад, оцінка кіберзахищеності для фінансової установи буде відрізнятись від оцінки для медичної установи. Невірне визначення сфери застосування може призвести до невірної оцінки рівня кіберзахищеності. При цьому на практиці часто не враховується ймовірності виникнення кіберзагроз та рівень потенційної шкоди від їх реалізації, що призводить до перенаправлення зусиль на менш значущі загрози [2].

Отже, визначення рівня кіберзахищеності об'єктів критичної інформаційної інфраструктури є складним завданням, яке потребує поєднання технічних, організаційних та людських аспектів. Для усунення зазначених проблем необхідно розробити загальноприйняту систему оцінки кіберзахищеності, яка буде їх враховувати. Це в свою чергу дозволить здійснювати адекватне визначення та ефективне порівняння рівнів кіберзахищеності між різними об'єктами.

Список використаних джерел та літератури

1. Грищук Р. Даник Ю. Основи Кібернетичної Безпеки. Монографія. Житомир : ЖНАЕУ, 2016. с.636.
2. Грищук Р. В., Охрімчук В. В. Напрямки підвищення захищеності комп'ютерних систем та мереж від кібератак // Актуальні питання забезпечення кібербезпеки та захисту інформації : тези доповідей учасників ІІ Міжнародної науково-практичної конференції. Київ : Видавництво Європейського університету, 2016. С. 60–61..
3. Охрімчук В. В. Метод побудови шаблонів потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення : дис. канд. техн. наук : 21.05.01 / Охрімчук Володимир Васильович – Житомир, 2021. – 170 с.