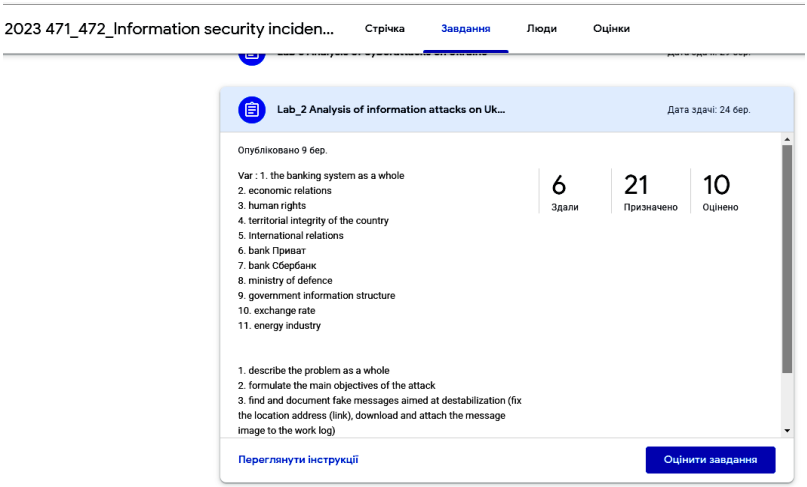

Рис. 1. Лабораторна робота Analysis of information attacks on Ukraine з дисципліни «2023 471_472_Information security incident management», НАУ, 2023 рік

Розробка навчально-методичних матеріалів, їх практична апробація та формування групи фахово-підготовленої молоді, вмотивованої на виявлення, моніторинг та фіксацію російської дезінформаційної діяльності є основними результатами цього року.

УДК 004.274:004.056

ВИКОРИСТАННЯ ПЛІС ДЛЯ ЗАХИСТУ КІБЕРФІЗИЧНИХ СИСТЕМ ЕНЕРГЕТИКИ

Сергій Гільгурт

ІПМЕ ім. Г.Є. Пухова НАН України, hilgurt@ipme.kiev.ua

Цировізація промислового обладнання та кіберфізичні системи останнім часом все частіше використовуються для підвищення ефективності критичної інфраструктури, зокрема, в енергетичній галузі. Цифровізація електричних підстанцій, які є найпоширенішими об'єктами електроенергетики, відбувається згідно низки стандартів МЕК-61850 «Мережі та системи зв'язку на підстанціях», згідно якого єдиним засобом передачі інформації на всіх рівнях підстанції прийнятий стандарт Ethernet. На жаль, пакетна передача даних і протоколи, що на ній засновані, роблять цифрові підстанції більш вразливими для кібератак. Наявний в ІТ-галузі досвід захисту інформації не може буди безпосередньо застосований до цифровізованих промислових систем, але з низкою поправок його доцільно використовувати. До дієвих засобів протидії загрозам безпеки інформації

відносяться сигнатурні засоби, зокрема, системи IDS/IPS, побудовані за сигнатурним принципом. Прискорити ресурсоємну процедуру множинного розпізнавання патернів в таких системах дозволяють апаратні пристрої на базі ПЛІС.

Метою даної роботи є дослідження можливостей та особливостей використання пристроїв програмованої логіки в якості апаратної платформи для побудови сигнатурних систем технічного захисту інформації в кіберфізичних системах енергетичної галузі.

В результаті аналізу існуючих кіберфізичних систем, знайдено два класи технічних засобів, що містять ПЛІС, на яких можуть бути реалізовані апаратні засоби захисту інформації. По-перше, це системи управління, що використовують такі інтелектуальні технології як нейронні мережі та нечітку логіку, інтелектуальні системи збору даних, частотні перетворювачі для електроприводів тощо. По-друге, деякі "розумні" електронні пристрої (Intelligent Electronic Devices – IED) , які також використовуються технологією Smart Grid кіберфізичних систем містять ПЛІС і системи на кристалі. Реконфігурація (оновлення обчислювальної структури) програмованих пристроїв може бути виконано віддалено. Проте даний процес необхідно захистити, оскільки канал зв'язку привносить потенційну вразливість у разі фізичного доступу зловмисника до мережі. В роботі розглянуто безпечний протокол і реконфігуровний модуль на ПЛІС, який використовується для налаштування та моніторингу мережевих IP-адрес. Запропонована полегшена версія протоколу другого рівня, реалізованого повністю апаратно та захищеного криптографічним алгоритмом AES-GCM відповідно до стандарту IEC 61850-90-5.

Висновки. ПЛІС, що задіяні в пристроях промислової автоматики, а також входять до складу інтелектуального цифрового обладнання, можуть бути використані для синтезу в них апаратних систем захисту інформації. Для безпечної віддаленої конфігурації ПЛІС, що використовуються в засобах захисту кіберфізичних систем, необхідно вживати додаткові заходи.

УДК 004.681.3

АЛГОРИТМ СТРУКТУРНОЇ ІДЕНТИФІКАЦІЇ ПРОГНОЗУЮЧИХ МОДЕЛЕЙ

[1]Хорошко Володимир Олексійович, [2]Хохлачова Юлія Євгенівна, [3]Вишневська Наталія Сергіївна

Національний авіаційний університет

[1]professor@ukr.net,

[2]yuliiahohlachova@gmail.com, [3]nataliia.vyshnevska@npp.nau.edu.ua

Прогнозування кіберзахищеності об'єктів є одним із вирішальних наукових факторів формування стратегії та тактики кіберзахисту.

Для прогнозування та моделювання процесів кіберзахисту найбільш прийнятними є статистичні методи, що ґрунтуються на існуючих тенденціях у змінах показників кіберзахищеності.