[Електронний ресурс] – Режим доступа к ресурсу: https://aws.amazon.com/ru/cloudformation/

## СТАНДАРТИЗАЦІЯ КРИПТОБЕЗПЕКИ ЗАДЛЯ ПОТРЕБ ТА ВИКЛИКІВ СЬОГОДЕННЯ

*Воргуль О.В., Білоцерківець О.Г.*

Харківський національний університет радіоелектроніки

*oleksii.bilotserkivets@nure.ua*

**Вступ.** В епоху Індустрії 4.0, коли машини апарати та станки підключені до мережі та між собою за допомогою смарт-пристроїв, масштаби та різноманітність кібератак зросли в геометричній прогресії. В такому взаємозв'язаному середовищі відомо, що порушення кібербезпеки можуть негативно вплинути на ефективність виробництва в цілому . Як доказ - дослідження, проведене Федерацією роботодавців машинобудування (EEF) щодо кібербезпеки показує, що з 48% виробників, які заявляють, що постраждали від кібератак, близько половини з них зазнали фінансових або інших промислових втрат.

**Мета дослідження.** Для вирішення питань кібербезпеки в Індустрії 4.0 вже розроблено значну кількість методологічних рішень. Однак не надто багато уваги приділяється аналізу критично важливих активів для захисту від кібератак та наслідків для організації. З іншого боку, такий аналіз у контексті мережевого виробництва може зіграти стратегічну роль для компаній, щоб зрозуміти, яким промисловим активам інвестувати свої зусилля з точки зору безпеки, в якому порядку та в якій мірі. З метою підтримки керівництва компанії у вирішенні таких питань кібербезпеки, у цьому дослідженні основна увага приділяється оцінці несприятливих наслідків для організації та її активів внаслідок порушень кібербезпеки мережевих виробничих машин.

Аналіз сучасного рівня техніки показав відсутність методології оцінки впливу, орієнтованої на глибоке розуміння та вагомість впливів у контексті Індустрії 4.0. Аналіз літератури запропонував деякі напрямки діяльності та прогалину, яку слід заповнити для підтримки компаній у здійсненні належних заходів щодо кібербезпеки.

Для того, щоб задовольнити мету дослідження та відповісти на питання дослідження, підхід NIST 800-30, розглядався як еталон для вирішення ризиків

кібербезпеки в 4,0 промислових контекстах. Підхід NIST має вихідну точку для оцінки ризиків ідентифікацію активів, на які впливають події загроз, та наслідки, які можуть виникнути, можливо, використовуючи результати аналізу впливу місії чи бізнесу та виявлення загроз, які спричиняють ці наслідки.

На основі доказів, зібраних у літературі, керівних принципів NIST та методу етнографічного дослідження, була визначена структурована класифікація критично важливих активів, що захищаються від кібератак та їхніх наслідків для бізнесу. Більше того, було встановлено взаємозв'язок між критичними активами та наслідками для бізнесу, а також методи оцінки впливу на бізнес

Для того, щоб оцінити вплив кіберзагроз на ефективність бізнесу, одним з основних моментів, на якому слід зосередитись, є характеристика основних активів, що підлягають захисту .

**Результати**. Посилаючись на результати огляду літератури, заснованого на характеристиці питань кібербезпеки в контексті Індустрії 4.0, кіберфізичні системи (CPS) та промислові системи управління (ICS) вважаються основними промисловими активи, що беруть участь у питаннях кібербезпеки. На ці системи може впливати низка вразливих місць, які потенційно можуть бути розміщені в усіх інтерфейсах між різними компонентами, де відбувається обмін інформацією. Наприклад, вразливості систем SCADA (які є підмножиною ICS) можуть стосуватися комунікаційної інфраструктури та мережевих протоколів, сервера додатків та сервера баз даних, машинних інтерфейсів, програмних логічних контролерів та віддалених термінальних блоків. Точно так само, оскільки сучасні підключені до Інтернету виробничі машини (наприклад, ті, що знаходяться у виробничій комірці) є розумними обчислювальними системами, що беруть участь у так званих операційних технологіях (OT), вони можуть мати такі вразливі місця:

•Операційні системи, що дозволяють працювати на машині;

•Прикладне програмне забезпечення (наприклад, програмне забезпечення САПР, CAM та CAE, програмне забезпечення управління машиною, інше програмне забезпечення загального призначення), що дозволяє машині виконувати свої робочі цикли відповідно до проектних, виробничих та технічних вимог.

•Промислові протоколи зв'язку (такі як MTconnect, Modbus, Profibus, EtherNet / IP та OPC-UA), які забезпечують цифровий обмін даними між машинними пристроями (датчиками та виконавчими механізмами) та іншими об'єктами / пристроями через мережу;

•Розумні пристрої (такі як датчики та пускачі), вбудовані в машини, які управляють потоком вхідних та вихідних даних через дротову або бездротову мережу.

Використання цих уразливостей за допомогою кібератак означає несанкціоновану дію на дані. Зокрема, дані можуть бути неналежним чином перехоплені (порушення конфіденційності даних), модифіковані або сфальсифіковані (порушення цілісності даних), або їх потік може бути перерваний (порушення доступності даних).

**Висновок.** На сьогоднішній день кібербезпека є одним з основних викликів, з якими доводиться стикатися компаніям, які наближаються до парадигми Індустрії 4.0, щоб зберегти свою конкурентоспроможність.

За останні роки європейські та міжнародні стандарти визначили стандарти та керівні документи, щоб створити спільне бачення засобів контролю кібербезпеки, необхідних у галузі, а також методів оцінки ефективності цих засобів контролю.

Управління кібербезпекою в Індустрії 4.0 також є новою та актуальною темою в останній літературі. Насправді, хоча аналіз літератури свідчить про те, що існує значна кількість методологічних рішень для вирішення питань кібербезпеки в контексті Індустрії 4.0, жодне з них не фокусується на питаннях безпеки, пов’язуючи критично важливі активи, що захищаються від кібератак та наслідків наслідки для бізнесу, забезпечуючи також їх значимість.

**Література.**

1. ST’s secure microcontrollers contribute to a smarter and more secure connected world [Електронний ресурс] / Режим доступу до ресурсу : https://www.st.com/en/secure-mcus/secure-hardware-platforms.html

2. The National strategy Industry 4.0 Асоціація підприємств промислової автоматизації України (АППАУ) [Електронний ресурс] / Режим доступу до ресурсу : https://appau.org.ua/en/category/pubs/