Проблеми цифровізації для систем Farming 4.0

В'юненко О.Б.*, *доцент*; Толбатов В.А.**, *доцент*;
Толбатов А.В.*, *доцент*
*Сумський національний аграрний університет, м. Суми, Україна
**Сумський державний університет, м. Суми, Україна

Розумне землеробство, також відоме як Farming 4.0 та цифрове землеробство - це застосування інформаційних систем (ІС) та інформаційних технологій (ІТ) для оптимізації складних систем землеробства. Інтеграція інтелектуальних сільськогосподарських технологій та сучасних технологій обробки даних дозволяє адаптувати посіви насіння до певної ділянки поля, щоб забезпечити ефективний виробничий процес. Застосування ІТ і технологій обробки даних допомагає сільгоспвиробникам у прийнятті обґрунтованих рішень на основі конкретних даних. Це відкриває шлях для того, щоб сільськогосподарські машини могли обмінюватися даними між собою. Існуючі системи управління сільськогосподарськими підприємствами, сільськогосподарські програми та Інтернет-платформи для підтримки виробників зараз вже включають не лише окремі машини, а й усі господарські операції на підприємствах. Виробники також можуть отримати доступ до даних у реальному часі на мобільних пристроях (смартфонах або планшетах), такі дані, як стан ґрунту та рослин, рельєфу місцевості, погоди, використання ресурсів, робочої сили, заявок на фінансування збираються, обробляються і оцінюються.

Незважаючи на те, що перспективи інтеграції технологій, практик та мислення в галузі сільського господарства в кінцевому підсумку є хорошими, їх прийняття потребує часу. Цей сектор виробництва стикається із значними проблемами - від стандартизації технологій до можливості інвестувати в модернізацію обладнання та допоміжну інфраструктуру підприємств. Цифровізація Farming 4.0 вимагає нових технологічних стандартів для забезпечення сумісності обладнання. Враховуючи тривалість життя с.-г. обладнання, стандарти є необхідністю для забезпечення того, щоб будь-який технологічний вибір залишався сумісним із новим обладнанням і підтримувався.

Тобто актуальною стає проблема розробки стандартів обміну даними та комунікації, які пов'язують різні системи в єдину інтегровану ІС, що охоплює всі аспекти с.-г. виробництва.

Проблеми уразливості кібербезпеки Industry 4.0

В'юненко О.Б.*, *доцент*; Толбатов В.А.**, *доцент*;
Толбатов А.В.*, *доцент*; Виганяйло С.М.***, *доцент*
*Сумський національний аграрний університет, м. Суми, Україна
**Сумський державний університет, м. Суми, Україна
***Сумська філія Харківського національного університету внутрішніх справ, м. Суми, Україна

Нова хвиля Industry 4.0 підштовхнула виробників швидше рухатися в напрямку цифрового перетворення, поміщаючи дані в хмару і використовуючи передові аналітичні засоби для поліпшення раніше непрозорих виробничих процесів. Для збору, агрегування та аналізу даних із застарілих промислових активів промислові компанії розміщують датчики та системи управління поверх існуючих технологій, це надає можливість приймати найкращі рішення щодо експлуатаційних та виробничих процесів, а також надає фінансовим командам краще уявлення про ефективність роботи та витрати на підприємстві. Негативною стороною Industry 4.0 є ризики, які вона створює для виробничих компаній. Більше заводських систем, які колись були досить закритими, тепер підключені до зовнішнього світу і в деяких випадках навіть доступні через Інтернет. Ризики в цьому цифровому світі набагато вищі, ніж в інших сферах. Основна проблема полягає в тому, що неможливо просто зупинити виробничу лінію або електростанцію, щоб переконатися, що всі системи працюють належним чином. Насправді будь-які зміни в системах управління, орієнтованих на виробництво, вважаються надзвичайно ризикованими, а промислові компанії навіть не хочуть застосовувати стандартні засоби сканування мережі та засоби виявлення вразливостей для своїх систем, боячись перевантажити мережі, вплинути на продуктивність та збільшити затримку систем зв'язку. Виробничі компанії прагнуть навчити свої команди оперативно реагувати на кібератаки за найбільш реалістичними сценаріями. Це означає доступ до нових способів запуску сценаріїв атак, аналогічних до тих збоїв контролю безпеки, які вони спостерігають у власних мережах. Найбільшою проблемою компаній є відсутність актуального кібер-досвіду по загрозам, з яким їхні команди можуть зіткнутися при реальних атаках на сучасні системи управління.