



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУГАНСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
ПРОЄКТ USAID «ЕКОНОМІЧНА ПІДТРИМКА СХІДНОЇ УКРАЇНИ»
ВІРМЕНСЬКИЙ ДЕРЖАВНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ТБІЛІСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНЕ
ДЖАВАХІШВІЛІ
ТАВРІЙСЬКИЙ ДЕРЖАВНИЙ АГРОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ДМИТРА МОТОРНОГО
ДОНБАСЬКА ДЕРЖАВНА МАШИНОБУДІВНА АКАДЕМІЯ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Збірник матеріалів
II Міжнародної науково-практичної конференції «Використання інформаційних технологій для оптимізації процесів виробництва сільськогосподарської продукції та управління підприємствами»
(Агро-ІТ)

10-11 березня 2022 р.
9-10 червня 2022 р.
(відтерміновано у зв'язку з військовою ситуацією, що сталась в Україні)



Дніпро-2022

МОГУТОВА В.Ф, БАКУМЕНКО Р.О. АНАЛІЗ ТЕХНОЛОГІЙ ВИРОБНИЦТВА ВАРЕНИХ КОВБАС ТА ШЛЯХИ УДОСКОНАЛЕННЯ.....	73
МОГУТОВА В.Ф, ЖЕЛУК А.Є. МОДЕЛЮВАННЯ СПОСОБІВ ВИРОБНИЦТВА МАСЛА ВЕРШКОВОГО	74
МОГУТОВА В.Ф, КОНСТАНТИНОВА М.К. РОЗРОБКА ТЕХНОЛОГІЙ СИРУ КИСЛОМОЛОЧНОГО ОЗДОРОВЧОГО ПРИЗНАЧЕННЯ	78
НЕДОСЄКОВА Н.С., РАЙ Д.В. АНАЛІЗ ВИНОРІБНОЇ ПРОМИСЛОВОСТІ УКРАЇНИ	80
СІЛЬЧЕНКО К.П, БОНДАРЕНКО А.С. УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ МОРОЗИВА.....	82
ШАХОВА Ю.Ю. ЕФЕКТИВНІСТЬ УДОСКОНАЛЕНОГО СПОСОБУ РОЗМОРОЖУВАННЯ СЕКСОВАНИХ СПЕРМОДОЗ	84
СЕКЦІЯ «ІНФОРМАЦІЙНІ СИСТЕМИ, ІНСТРУМЕНТАРІЙ ТА ТЕХНОЛОГІЙ В МАРКЕТИНГОВІЙ ДІЯЛЬНОСТІ ПІДПРИЄМСТВ АПК»	86
АНДРЮХІН О.О., МІНАКОВА В.О. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЙ В МАРКЕТИНГОВІЙ ДІЯЛЬНОСТІ ПЕРЕРІБНОГО ПІДПРИЄМСТВА.....	86
БАЛДИК Д.О. ТЕНДЕНЦІЙ ЕКОНОМІЧНОГО РОЗВИТКУ З УРАХУВАННЯМ ПОТЕНЦІАЛУ ЛЮДСЬКОГО КАПІТАЛУ	90
БЕРЕЖНА Ю.Г., НАУМЕНКО І. В. МАРКЕТИНГОВІЙ МОНІТОРИНГ В УМОВАХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ.....	93
БРАСЛАВСЬКИЙ Д.В., БАЛДИК Д.О. КІБЕРБЕЗПЕКА ПОТРЕБУЄ КВАЛІФІКОВАНИХ ФАХІВЦІВ	96

Браславський Д.В., Балдик Д.О.

КІБЕРБЕЗПЕКА ПОТРЕБУЄ КВАЛІФІКОВАНИХ ФАХІВЦІВ

Луганський національний аграрний університет (м. Слов'янськ, Україна)

Комп'ютерна безпека – це сукупність методів захисту у галузі телекомунікацій та інформатики, пов'язаних з оцінкою та контролюванням ризиків, що виникають при користуванні комп'ютерами і комп'ютерними мережами, а також їх впровадження з точки зору конфіденційності, цілісності та доступності. Систему кібербезпеки України формує в тому числі і академічна кібербезпека (ЗВО, дослідницькі інститути і т.д.). Чому це важлива сфера в укріпленні держави казати не треба, бо навіть президент США Байден оголошував кібербезпеку головним питанням для своєї країни у жовтні 2021 року [1]. На рівні міждержавних відносин Україна-США домовились про проведення засідання щодо питань кібербезпеки [2]. Багато іноземних ЗМІ повідомляло, що фахівці з кібербезпеки США та Великобританії направлялись до України аби допомогти нашим співробітникам у цій справі [3]

Україна як держава розробила стратегію по кібербезпеці [4] Проте фахівці з кібербезпеки мають з'являться саме з українських ЗВО. Частина з цих закладів є військовими, як наприклад Військовий інститут телекомунікацій та інформатизації Державного університету телекомунікацій [5] або Житомирський військовий інститут імені С. П. Корольова [6]. Частина не мають військового ухилу, як наприклад Донецький національний технічний університет [7] або Київський національний економічний університет ім. Вадима Гетьмана [8]. Загалом, із публічних джерел стає відомо про мінімум 61 ЗВО, який готує фахівців із кібербезпеки [9]. Частина із цих ЗВО є приватними закладами.

Досі існує тенденція дефіциту фахівців у цій сфері. За словами експерта (ІТ-бізнесмен та інвестор у сфері інформаційної та кібербезпеки, голова наглядової ради "Октава Капітал" Олександр Кардаков, обладнання за мільйони

доларів саме по собі не захистить цифрові дані від атаки, оскільки технічні засоби й процеси не забезпечують наскрізного моніторингу подій: їх або недостатньо, або вони неправильно експлуатуються, або немає кваліфікованих фахівців, які в наборі, на перший погляд, непов'язаних подій зможуть відстежити атаку. Він також зазначив, що до топ нових кіберзагроз у 2021 році входять Advanced Persistent Threats – так звані таргетовані атаки, кількість яких збільшилася на 60% із моменту початку пандемії, а також атаки з виманням, про які на прикладах Colonial Pipeline, Acer, Cd Projekt, Kia Motors і багатьох інших дізнався весь світ [10].

Вирішення цих проблем має мати комплексний характер:

- залучення до роботи представників Міністерства освіти і науки України, Міністерства цифрової трансформації України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України та Департаменту кіберполіції Національної поліції України;
- впровадження дуальної освіти у даних державних структурах могли би втримати здобувачів саме на цих робочих місцях, бо більшість з них в процесі здобування освіти або після її завершення переходять працювати у приватні структури;
- залучення до роботи у таких структурах іноземних фахівців, які б могли надавати величезний досвід нашим здобувачам;
- посилення на рівні держави інтеграції з міжнародними інституціями (по прикладу НАТО), впровадження нових практик;
- збільшення фінансування відповідних підрозділів, органів влади які відповідають і за кібербезпеку, і за процес навчання фахівців з кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кібербезпека стане головним питанням для США в жовтні – Байден [Електронний ресурс]. – Режим доступу: <https://www.ukrinform.ua/rubric->

world/3325206-kiberbezpeka-stane-golovnim-pitannam-dla-ssa-v-zovtni-bajden.html

2. Україна та США домовились про зустріч щодо кібербезпеки /Ярослав Прищепка // [Електронний ресурс]. – Режим доступу: <https://suspilne.media/160326-ukraina-ta-ssa-domovilis-pro-zustric-sodo-kiberbezpeki/>

3. США та Велика Британія відправили до України фахівців з кібербезпеки – ЗМІ /Олексій Кравченко // [Електронний ресурс]. – Режим доступу: <https://glavcom.ua/country/society/ssha-ta-velika-britaniya-vidpravili-do-ukrajini-fahivciv-z-kiberbezpeki-zmi-808360.html>

4. Указ президента України №447/2021 [Електронний ресурс]. – Режим доступу: <https://www.president.gov.ua/documents/4472021-40013>

5. Військовий інститут телекомунікацій та інформатизації Державного університету телекомунікацій (БІТІ ДУТ) [Електронний ресурс]. – Режим доступу: <http://osvita.ua/vnz/guide/48/>

6. Житомирський військовий інститут імені С. П. Корольова (ЖВІ) [Електронний ресурс]. – Режим доступу: <http://osvita.ua/vnz/guide/229/>

7. Донецький національний технічний університет (ДонНТУ) [Електронний ресурс]. – Режим доступу: <http://osvita.ua/vnz/guide/135/>

8. Київський національний економічний університет ім. Вадима Гетьмана (КНЕУ) [Електронний ресурс]. – Режим доступу: <http://osvita.ua/vnz/guide/69/>

9. Довідник ВНЗ [Електронний ресурс]. – Режим доступу: <http://osvita.ua/vnz/guide/search-17-0-0-42-0.html/>

10. Дефіцит кадрів на ринку кібербезпеки в Україні загострюється - думка [Електронний ресурс]. – Режим доступу: <https://ua.interfax.com.ua/news/telecom/753998.html>