УДК 378:336:004.49:005.93

Биков Валерій Юхимович
доктор технічних наук, професор, академік НАПН України, директор
Інститут інформаційних технологій і засобів навчання НАПН України, м. Київ, Україна
ORCID ID 0000-0002-5890-6783
valbykov@gmail.com

Романовський Олександр Олексійович
доктор педагогічних наук, доктор економічних наук, професор, ректор
Українсько-американський університет Конкордія, м Київ, Україна
ORCID ID 0000-0002-3618-2999
oleksandr.romanovskyi@uacu.edu.ua

Романовська Юлія Юріївна
кандидат філологічних наук, професор, віце-ректор
Українсько-американський університет Конкордія, м Київ, Україна
ORCID ID 0000-0002-0207-3348
yuliia.romanovska@uacu.edu.ua

НАВЧАННЯ КІБЕРБЕЗПЕКИ І КІБЕРЗАХИСТУ ФАХІВЦІВ З УПРАВЛІННЯ ФІНАНСАМИ, ЕКОНОМІКОЮ І БІЗНЕСОМ

Анотація. Дослідження присвячене незвичайно актуальній темі підвищення кіберграмотності населення. Дослідження базується на унікальному досвіді міжнаціонального навчального проєкту «Основи корпоративної кібербезпеки». Мета даної роботи – запропонувати підхід до вирішення проблеми підготовки громадян України (і, можливо, громадян інших країн) до протидії кіберзагрозам у їх професійній діяльності. Об'єкт дослідження – фінансова індустрія, яка є частиною програм старших класів/курсів коледжів і університетів багатьох країн. Автори висувають таку ідею: щоб навчити основам кібербезпеки неспеціалістів у сфері ІТ – тих, хто не має спеціальної інженерно-технічної підготовки в галузі ІТ і кіберзахисту, і фахівців у сфері соціального захисту – економічна сфера (бізнес-лідери, підприємці, економісти, фінансисти і ін.) необхідно навчати кібербезпеці, орієнтованій на їх професійну діяльність. У результаті проведених досліджень авторами визначено, що в багатьох країнах, особливо в країнах, що розвиваються, кіберзлочинність є серйозною проблемою. Автори доводять, що Україні необхідно інтенсивне навчання громадян усіх вікових груп проблемам фінансових злочинів і шахрайства з боку інтернет-хакерів і кіберзлочинців. Поряд з професійною підготовкою фахівців у сфері інформаційних технологій і кібербезпеки в Україні доцільно: запровадити в шкільній системі навчання домашнім фінансам і методам їх ІТ захисту; навчати основам інформаційних технологій, кібербезпеки, фінансів і економіки в усіх коледжах, інститутах і університетах; організувати навчання у сфері інформаційних технологій і кібербезпеки для громадян України. Для забезпечення інтеграції України з Європою тісна співпраця з розвиненими країнами та транснаціональними організаціями має вирішальне значення для розвитку процвітаючого сектора кібербезпеки. В Україні достатньо грамотних молодих фахівців у галузі ІТ, які успішно працюють на закордонні компанії та корпорації. Для ефективного використання цього людського ресурсу доцільно створити координуючий навчальний центр з кібербезпеки у сфері економічної і фінансової діяльності.

Ключові слова: кіберзагроза; кібератака; кібершахрайство; кіберзахист бізнесу і фінансів; навчання корпоративної фінансової кібербезпеки.

1. ВСТУП

Сьогодні людство переживає бурхливу інформаційну революцію, пов'язану з формуванням, розвитком і поширенням транскордонних глобальних інформаційно-телекомунікаційних мереж, що покривають усі країни і континенти, проникають до кожного будинку і які одночасно впливають на кожну людину окремо і на величезні маси людей.

Найбільш яскравим прикладом такого явища і його результатом є Інтернет. Суть цієї революції полягає в інтеграції в єдиному інформаційному просторі по всьому світу програмно-технічних засобів, засобів зв'язку і телекомунікацій, інформаційних запасів або запасів знань як єдиної інформаційної телекомунікаційної інфраструктури, у якій активно діють юридичні та фізичні особи, органи державної влади та місцевого самоврядування. У результаті неймовірно зростають швидкості і обсяги оброблюваної інформації, з'являються нові унікальні можливості виробництва, передачі і поширення інформації, пошуку і отримання інформації, нові види традиційної діяльності в цих мережах.

Розпочата в 2012 році Четверта промислова революція, викликана необхідністю конкурентоспроможності обробної промисловості за допомогою посиленої інтеграції та впровадження «кіберфізичних систем» у виробництво (Індустріальна Революція 4.0 або 4IR) і обслуговування таких людських потреб, як побут, праця і дозвілля, стрімко завершується. Уже близька П'ята промислова революція (5IR).

Як проаналізовано в роботі [1], експерти, науковці та філософи всього світу намагаються визначити, що стане поштовхом до початку П'ятої промислової революції. Чи буде це революція штучного інтелекту (майже те саме, що і Індустріальна Революція 4.0)? Чи буде це пов'язано з потенціалом квантових обчислень? Компанія ж Genpact передбачає, що «люди і машини об'єднаються на робочому місці» [2]. Можливо, ближче до істини став вислів засновника Salesforce Марка Бениоффа: «Настає криза довіри до технологій. Під час п'ятої промислової революції нам знадобиться головний спеціаліст з етики та гуманності. Ви не можете вести бізнес в Четвертій промислової революції без довіри ваших співробітників, клієнтів і партнерів» [3]. Швидше за все, Четверта і П'ята промислові революції відбудуться паралельно, водночас 5IR визначатиме етику і вплив технології, розробленої в четвертій. Клаус Шваб, засновник і глава Всесвітнього економічного форуму (ВЕФ), вважає, що зараз ми знаходимось на переломному етапі. Ключові зрушення в технологіях, що розглядаються як «світ завтрашнього дня», відбудуться в наступному десятилітті [4], Також ВЕФ прогнозує, що технології, які імплантуються, будуть широко поширеними до 2023 року, 3D-друк – до 2022 року, штучний інтелект (ШІ) замінить людей на багатьох робочих місцях до 2025 року і стане спроможним приймати важливі рішення – до 2026 року.

На людство чекає серія винаходів, які кардинально змінять його спосіб життя [5]. Можливо, що до 2055 року половина всієї роботи у світі буде автоматизована. Домінік Прайс, глобальний робочий футурист з Atlassian, поділився з Metro.co.uk своїми припущеннями про те, що: «Головний плюс для працівників і роботодавців полягає в тому, що ШІ, швидше за все, відмовиться від вельми повторюваних і звичайних завдань, які повинні звільнити нас, людей, для виконання більш значущою роботи, що включає творчість, цікавість, співчуття і судження» [1].

Постановка проблеми. Ера загальної інформатизації, автоматизації, роботизації і всього, що стосується сфери ШІ, має як позитивні сторони (підвищення продуктивності праці, заміну людини в небезпечних професіях, високу швидкість прийняття рішень і

реагування), так і суттєві негативні, і навіть небезпечні для існування людства сторони. Це, у першу чергу, небезпека кібератак, що використовуються як засоби гібридних воєн, які вражають оборонну здатність і економіки країн, руйнують їх банківсько-фінансові системи, відбирають шахрайськими способами кошти підприємств і заощадження громадян. Необхідність протистояння кібератакам супротивників і шахраїв є пріоритетною практично для всіх країн світу й України зокрема [6], [7]. Багато НДІ і ЗВО України займаються питаннями розробки адекватних методів протистояння кібератакам, а також підготовкою фахівців у цій сфері. Тому необхідне значне державне фінансування, пов'язане як з технічними питаннями, так і підготовкою необхідного контингенту фахівців належної кваліфікації.

Завданням даної роботи є спроба запропонувати часткове вирішення проблеми підготовки громадян України (а, можливо, і інших країн) до протистояння кіберзагрозам у своїй професійній діяльності. Об'єктом дослідження обрано галузь фінансів, теми якої містяться в програмах старших класів середніх шкіл, коледжів і університетів багатьох країн світу.

Авторами роботи була висунута ідея про те, що фахівців соціально-економічної сфери (керівників бізнесу, підприємців, економістів, фінансистів та ін.) необхідно навчати основам кібербезпеки і кіберзахисту, орієнтованих на їх професійну діяльність.

Авторами було обрано конкретну навчальну програму підготовки бакалаврів у сфері бізнес-адміністрування (Bachelor of Business Administration Program), яка викладалась онлайн навесні 2020 року в Українсько-американському університеті Конкордія (УАУК). У межах цієї програми студентам УАУК і багатьом бажаючим з України та інших країн світу англійською мовою викладався спеціальний курс «Основи корпоративної кібербезпеки» ("Essentials of Enterprise Cyber Security").

Аналіз останніх досліджень і публікацій. Сьогодні існує величезна кількість досліджень і публікацій, присвячених кібербезпеці, кіберзлочинності і статистиці фінансових злочинів за допомогою ІТ. Найбільший внесок у розслідування фінансових злочинів вносить ФБР, яке є провідною федеральною агенцією США з розслідування зловмисної кіберактівності злочинців, ворогів національних держав і терористів. Центр скарг щодо інтернетзлочинів ФБР (IC3), створений у 2000 р, має надійний і зручний механізм для надання громадськості інформації про підозрювану злочинну діяльність, пов'язану з Інтернетом. У кінці кожного року IC3 об'єднує інформацію, зібрану до річного звіту. Так, у звіті за 2019 г. [8], наведена статистика скарг і фінансових втрат по всьому світу в 2015-2019 роках (табл. 1):

Таблиця 1

Статистика скарг і фінансових втрат по всьому світу в 2015-2019 роках

Роки	Загальна кількість скарг	Загальні фінансові втрати
2015	288 012	1,1 млрд. дол. США
2016	298 728	1,5 млрд. дол. США
2017	301 580	1,4 млрд. дол. США
2018	351 937	2,7 млрд. дол. США
2019	467 361	3,3 млрд. дол. США
Усього:	1 707 618	10,2 млрд. дол. США

За майже 20 років існування IC3 у 2019 році було зареєстровано найбільшу кількість

скарг і найбільшу кількість заявлених втрат. Так, за даними звіту [9], у міжнародному масштабі США випереджають решту країн світу за повідомленнями щодо злочинності в Інтернеті (467 361). У Сполученому Королівстві було трохи більше 93 700 жертв. Канада була наступною в списку з більш ніж 3700 скаргами.

Відзначимо, що величини канадських і британських цифр значно менші в порівнянні з кількістю населення Канади і Британії. Це пов'язано з тим, що класифікація кіберзлочинів може бути різною. Крім того, різним є і характер використання ідентифікаційних номерів громадян у США, Канаді і Британії.

Кількість людей, які постраждали від кіберзлочинності в 2019 році, була вище ніж будь-коли. І сума втрат була значною. У всьому світі, за оцінками, від 3,3 до 3,5 млрд. доларів було втрачено приватними особами або підприємствами протягом року. Шлях отримання цих грошей є різноманітним. Використовуючи соціальні мережі, шахраї отримали доступ до більш ніж 78 775 000 доларів. Втрати віртуальної валюти склали більше 159 329 000 доларів.

Звіти IC3 дозволяють зрозуміти, хто найбільше страждає від онлайн шахраїв і кіберзлочинів. Люди старші за 60 років складають більшість із понад ніж 68 тис. жертв. Загальні втрати для цієї вікової групи склали понад 835 млн. дол. США. З віком збільшується і кількість жертв. Однак навіть у наймолодшій групі віком до 20 років зареєстровано понад 10, 7 тис. жертв, разом вони втратили понад 421 млн. дол. США. Це підтверджує той факт, що IC3 намагається задекларувати, що будь-яка людина на будь-якому етапі життя може стати жертвою кібератаки, і водночас злочинці стають більш досвідченими і витонченими. У табл. 2 наведено статистику жертв і їх фінансових втрат в 2019 році за віковими групами [9].

Таблиця 2

Статистика жертв і їх фінансових втрат в 2019 році за віковими групами

Вікова група	Загальна кількість жертв	Загальні фінансові втрати
До 20 років	10 724	421 169 232 дол. США
20-29 років	44 496	174 673 470 дол. США
30-39 років	52 820	332 208 189 дол. США
40-49 років	51 864	529 231 267 дол. США
50-59 років	50 608	589 624 844 дол. США
Більше 60 років	68 013	835 164 766 дол. США
Усього :	278 525	2 882 071 768 дол. США

Не тільки приватні особи, але й великі фінансові установи стають жертвами кібершахрайства. Так, у липні 2019 року банк Capital One з популярним бізнесом по випуску кредитних карток, головний офіс якого перебуває у Вірджинії, оголосив, що хакер викрав близько 100 мільйонів заявок на кредитні картки, також були викрадені тисячі номерів соціального страхування і банківських рахунків. Дана хакерна атака є одним з найбільших зломів даних, що коли-небудь трапилися з фінансовими фірмами. Збиток від злому банк оцінює від 100 до 150 млн. доларів. Витік даних зачепив близько 100 млн. людей у США і близько 6 млн. у Канаді. У 2017 році кредитно-звітна компанія Equifax розкрила, що хакери викрали особисту інформацію 147 мільйонів громадян [10].

«Хоча я вдячний за те, що злочинець був спійманий, мені дуже шкода, що таке сталося», – заявив Річард Д. Фербенк, голова і виконавчий директор Capital One. «Я щиро

перепрошую за зрозуміле занепокоєння, яке цей інцидент має викликати в постраждалих, і я сповнений рішучості зробити це правильно». Багато експертів і журналісти вважають: ***«Все, що ви знали про створення надійних паролів, невірно»*** [11].

В останніх звітах про дослідження асоціації фахівців з кібербезпеки [12], надано невтішні прогнози щодо розширення кіберзлочинів у світі, наприклад:

- ✓ Збиток від кіберзлочинності до 2021 року буде обходитися світу в 6 трильйонів доларів на рік у порівнянні з 3 трильйонами доларів в 2015 році.
- ✓ До 2021 року на глобальні витрати на вимагання досягнуть 20 мільярдів доларів США.
- ✓ До 2021 року буде створено 3,5 млн. незайнятих робочих місць з кібербезпеки в порівнянні з 1 млн., відкритих у 2014 році
- ✓ Глобальні витрати на продукти і послуги кібербезпеки в сукупності перевищать 1 трлн дол. США з 2017 по 2021 рік
- ✓ Жінки становлять 20 відсотків працівників кібербезпеки в 2019 році та їх кількість буде постійно збільшуватися.
- ✓ До 2021 року понад 70% всіх транзакцій криптовалюти будуть відбуватись у сфері незаконної діяльності.
- ✓ До 2027 року глобальні витрати на навчання співробітників служб інформаційної та кібербезпеки будуть досягати 10 млрд. доларів.
- ✓ До 2022 року число користувачів Інтернету складе 6 мільярдів, а до 2030 року їх буде вже більше 7,5 мільярдів доларів США.
- ✓ До 2022 року глобальні витрати на продукти і послуги управління ідентифікацією та доступом (IAM) перевищать 16 мільярдів доларів США в рік. Водночас IAM все більше орієнтується на бізнес і вимагає ділових навичок, а не тільки технічних знань.

Необхідно відзначити, що переважна більшість кібератак і кібершахрайства відбувається в сфері фінансової діяльності товариства. Так, наприклад, Світовий банк (СБ) заявив, що за даними Групи 7 (G7) (2016 р.), ризики кібербезпеки для світової фінансової системи викликають серйозну стурбованість. Атаки на кіберпростір, тобто простір між взаємопов'язаними комп'ютерами, «стають все більш витонченими, частими і постійними, а кіберризики стають все більш небезпечними і різноманітними, погрожуючи порушити наші взаємопов'язані глобальні фінансові системи і інститути, які працюють і підтримують ці системи».

Так само Міжнародна Організація комісій з цінних паперів (IOSCO) (2016 р.) «визнала, що кіберризик є зростаючою і значною загрозою цілісності, ефективності і надійності фінансових операцій ринків по всьому світу» [13]. У 2019 році групою СБ було опубліковано «Глобальна програма щодо потенціалу кібербезпеки. Отримані уроки та рекомендації з посилення Програми.» [14], у якій зазначено, що на цей час понад три чверті інвестиційних проєктів Світового банку пов'язані з фінансуванням цифрових технологій, очікується, що ця частка з часом буде збільшуватися. Також підкреслюється, що Четверта промислова революція розгортається повним ходом і спонукає уряди оптимізувати існуючі IT-системи, впроваджуючи нові технології для реінжинірингу процесів, а також для надання нових державних послуг. Хмарні обчислення, ШІ, аналіз великих даних і нові технології змінюють методи роботи державних систем, що відповідають за управління державними фінансами, управління персоналом і надання державних послуг. Оскільки «перехід на цифрові технології» допомагає підвищити ефективність і скоротити витрати, інші урядові системи також можуть наслідувати їх

приклад. Проте є застереження щодо швидкої оцифровки, яка часто є результатом державних інвестиційних проєктів. Деякі з відчутних переваг цифрових технологій компенсуються виникаючими ризиками. Зокрема не можна ігнорувати ризик кібербезпеки, оскільки він може вплинути на життя, активи, довіру і соціальну стабільність, якщо не буде попереджений або ефективно пом'якшеним. Уразливість державних ІТ-систем, які піддаються впливу кіберпростору навіть протягом короткого періоду часу, можуть призвести до значних фінансових втрат і зловмисне вторгнення в систему державного управління з далекосяжними наслідками. Брак державних ресурсів, обізнаності та можливостей посилює цю проблему і часто є серйозною проблемою [14].

Українські експерти та фахівці в галузі інформаційної безпеки та кіберзахисту останнім часом опублікували ряд робіт, що викликають як суспільний інтерес, так і стурбованість станом справ у сфері національної кібербезпеки. Так, у роботі [15] відзначається, що статистика окремих банків показує: у 2019 році кількість кіберзлочинів збільшилась у 2,5-3 рази порівняно з 2018 роком. Небезпечну тенденцію щодо збільшення ризику шахрайства та кіберзагроз у банківській галузі показали останні опубліковані НБУ результати опитування, проведеного серед керівників банківських і небанківських фінансових установ, про системні ризики фінансового сектора. Фактор шахрайства і кіберзагроз за своєю значимістю тільки за кілька місяців 2019 року перемістився з 5 місця на 2. Якщо ще в травні 2019 року 54% респондентів, які пройшли опитування НБУ, вважали шахрайство і кіберзагрози високим або дуже високим фактором небезпеки, то вже в кінці 2019 року таким його вважали 70% опитаних. Вище за нього – тільки корупція.

У публікації [16] відзначається, що в суспільстві існує помилкова думка, що масові кібератаки здійснюються тільки на великі компанії: малі та середні підприємства отримують більш значної шкоди внаслідок кібератак у порівнянні зі збитками, з якими стикається великий бізнес в аналогічних ситуаціях. Середній відсоток доходу, який втрачають малі і середні підприємства через кібератаки, становить 3,4%. Водночас для великого бізнесу цей показник ледь сягає 0,05%.

Стаття [17] розглядає проблеми уникнення фішингу – одного з найпоширеніших способів інтернет-шахрайства. Підкреслюється, що часто люди не розуміють, що можуть втратити всі гроші просто через те, що полінувались поставити на свій Інтернет-банкінг пароль, відмінний від тих, які використовуються на інших акаунтах.

Більш повному огляду списку професійних публікацій у галузі інформаційного та кіберзахисту у світі присвячена робота [18].

Навчанням принципам і методам інформаційної та кібербезпеки займається ряд провідних ЗВО України. Однак вивченню кібербезпеки учасниками освітнього процесу присвячено не так багато досліджень. Однією з небагатьох є робота [19], у якій розглянуті проблеми кібербезпеки учасників освітнього процесу, акцентується увага на тому, що ці проблеми не зводяться тільки до технічних аспектів захисту інформаційних ресурсів, в повному обсязі, а й охоплюють різноманітні види захисту: правові, технічні, інформаційні, організаційні та психологічні. Складовою підготовки учасників навчального процесу з питань кібербезпеки пропонується використовувати «кібервакцинацію», тобто формування усвідомленого чуттєвого досвіду перебування під дією кіберзагрози і протидію їй системою заходів, які охоплюють, крім традиційних методів, тренувальні «кібератаки», а також формування знань і вмінь стійкості (відновлення) щодо кіберзагроз. Також пропонується подальші дослідження проблеми зосередити на детальній розробці структури загроз та методам протидії. Особливе місце повинна зайняти проблематика стійкості до кіберзагроз, яка може використовувати досвід підготовки операторів

емерджентних галузей, зокрема діагностування поточного стану людини і необхідної його корекції з метою оптимізації діяльності.

Однак, опублікованих матеріалів з наукових досліджень у галузі з навчання методам і засобам кіберзахисту для учнів і студентів інших спеціальностей, безпосередньо не пов'язаних з професіями в сфері ІТ і кібербезпеки, ще зовсім недостатньо. Особливо для навчання або професійної діяльності професіоналів у галузі бізнес-адміністрування, підприємництва, фінансів, бухгалтерського обліку та аудиту майже немає програм та виробленої методики навчання їх основам інформаційного та кіберзахисту.

Мета статті. З огляду на вищевикладене та загрозливу статистику зростання кіберзлочинів у сфері фінансово-економічної та господарської діяльності в житті людського співтовариства, автори пропонують розгляд низки підходів до підвищення рівня обізнаності та подальшої освіченості населення стосовно проблем реальної кібернебезпеки. А також – до навчання студентів, професіоналів і управлінців у сфері соціально-економічної та адміністративно-господарської діяльності теорії корпоративного кіберзахисту та протистояння кіберзагрозам на робочому місці і в повсякденному житті.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Теоретичною основою дослідження є NISTIR Стандарти кібербезпеки [20] – методи, зазвичай викладені в опублікованих матеріалах, які допомагають захистити кіберсередовище користувача або організації – мережі передачі даних, взаємозв'язок відкритих систем і безпеку [21]. До цього середовища належать самі користувачі, мережі, пристрої, усе програмне забезпечення, процеси, інформація у сховищі або при передачі, програми, служби та системи, які можуть бути прямо або побічно підключені до мереж.

Основною метою Стандартів кібербезпеки є зниження ризиків разом із запобіганням але, головним чином, – пом'якшення кібератак. Ці опубліковані матеріали складаються з наборів інструментів, політик, концепцій безпеки, заходів безпеки, посібників, підходів до управління ризиками, дій, навчання, кращих практик, гарантій і технологій.

Важливим аспектом кіберзахисту та кібербезпеки є юридичне регулювання щодо створення та впровадження ІТ та програмного забезпечення кібербезпеки компаній [22].

Також в основу дослідження покладена система теоретичної і практичної підготовки бакалаврів і магістрів за спеціальністю бізнес-адміністрування (Business Administration), прийнята в ЗВО США, України та багатьох країн світу.

3. МЕТОДИКА ДОСЛІДЖЕННЯ

Методика дослідження базується на емпіричному методі – вивченні і порівнянні достовірних світових і українських фактичних і статистичних даних, опублікованих в авторитетних джерелах, аналізі даних реальних кіберзлочинів і інтернет-шахрайства у сфері ведення бізнесу і фінансової діяльності. Під час роботи з фактичними даними і запропонованими авторами положеннями використовувались аналіз і синтез, індукція і дедукція, а також – уявне ситуативне моделювання. Також проведено дослідне навчання курсу основ корпоративної кібербезпеки студентів соціально-управлінського профілю, які не є профільними фахівцями в сфері інформаційно-комп'ютерних систем, інформаційного захисту та кібербезпеки.

4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У весняному семестрі 2019-2020 навчального року в онлайн режимі студенти УАУК спеціальності «бакалавр в сфері бізнес-адміністрування» та інших спеціальностей, а також бажаючі з України та інших країн прослухали англійською мовою курс з основ корпоративної кібербезпеки. Така можливість була запропонована в межах експериментального (пілотного) проєкту. Студенти і слухачі мали можливість не тільки прослухати лекції, а взяти участь у вебінарах, виконати практичні завдання, пройти онлайн тестування і отримати залікові бали з основ корпоративної кібербезпеки.

Основою цього експериментального проєкту стала ідея щодо кіберзахисту фінансово-економічної сфери України шляхом зменшення кіберфінансових злочинів. Розвиток культури кібернетичних та інформаційних технологій для загальної і стратегічної безпеки України повинен початися з розробки та впровадження навчання з питань зменшення кіберфінансових злочинів для галузевого керівництва і керівників підприємств. З огляду на те, що існує відсутність злиття дисциплін кібербезпеки, бухгалтерського обліку та аудиту, а також навчальних програм, які могли б надаватися галузевим керівникам та керівникам підприємств і бізнесу України, є нагальна потреба у створенні програм з професійного навчання та вивчення передового досвіду в сфері пом'якшення кіберфінансових злочинів. Такі програми будуть корисними для багатьох зацікавлених сторін: наукових кіл, галузевих установ і підприємств, компаній з комерційного бізнесу, ЗВО тощо.

Також важливо розглядати кіберфінансові злочини як прикладні наукові дослідження, виробляти механізми і методи вирішення проблем кіберфінансових злочинів. Цікавими і корисними є ініціативи країн ЄС, США, Великої Британії, Канади та інших економічно розвинених країн з надання знань, методів і протоколів у сфері кібербезпеки усім зацікавленим сторонам, щоб вони знали, розуміли та ефективно використовували кіберпростір для просування і захисту своїх підприємств.

Навіщо в Україні розглядати кіберфінансові злочини як провідну тему з безлічі тем в кібербезпеці? Тому що кіберфінансові злочини здійснюють безпосередній негативний вплив на керівників усіх ланок господарської та фінансової діяльності України. Поки що навчання і діяльність у сфері кібербезпеки майже повністю призначені лише для фахівців з ІТ-безпеки – персоналу, що володіє технічними навичками для захисту від кібератак за допомогою технічних засобів організації.

Однак, як показано у звіті PricewaterhouseCoopers 2018 в України [23], кібернетичні інструменти та кібербезпека практично не переводяться з технічної сфери в сферу, яку менеджери і керівники можуть застосовувати у своїй фінансовій сфері. Дисципліна «Кіберфінансові злочини» повинна надати керівникам усіх ланок засоби для застосування ефективних кіберінструментів і передових кіберпрактик для забезпечення обліку (рух грошових коштів) і аудиту (прозорість).

Які установи в сучасному світі можуть змінити рівень ***знань***, ***навичок*** і ***відносин*** управлінського класу?

Існує три ключових механізми інституційних змін:

- ✓ Вища освіта (університети, інститути, коледжі).
- ✓ Професійні навчальні заклади, такі як, наприклад, Інститут SANS (офіційно Інститут передових технологій Escal), який є приватною комерційною компанією США, заснованою в 1989 році, яка спеціалізується на інформаційній безпеці, навчанні кібербезпеки і сертифікуванні фахівців інформаційної та кібербезпеки.

- ✓ Професійні асоціації (Торгові палати, Інститути управління проєктами, Асоціація безпеки інформаційних систем і Асоціації фахівців з кібербезпеки).

В Україні, як і в багатьох країнах світу, проблемам інформаційної та кібербезпеки навчають у багатьох провідних ЗВО. Однак, сучасне професійне співтовариство з навчання кібербезпеки робить акцент на технічні засоби. Якщо такий поділ дисциплін продовжиться, вищим керівникам та керівникам різних ланок українських підприємств буде складно створити культуру кібербезпеки і протистояти кіберзагрозам та інтернет-шахрайству в сфері фінансової діяльності. Доцільно проаналізувати дані по кіберзлочинам і з фінансових втрат у світі за період з 2001 по 2019 роки [24].

Очевидно, що підхід до зміни рівня знань, навичок і відносин до інформаційної та кібербезпеки в сфері фінансів керівників середньої ланки і фахівців у галузі фінансів, економіки і управління господарською діяльністю є найбільш ефективним способом перетворення суспільного знання і ставлення до таких небезпечних загроз. Це можна пояснити тим, що:

- ✓ По-перше, керівники середньої і вищої ланки – це люди, що володіють відповідними посадами і повноваженнями для впровадження практики кібербезпеки.
- ✓ По-друге, вони мають компетенцію, знання і досвід для оцінки вартості і зважування витрат.
- ✓ По-третє, вони впливають як на свої кадрові ресурси – робочу силу, складову більшість у суспільстві, – так і на своїх безпосередніх керівників, які створюють і приймають законодавчі акти для впровадження кібербезпеки і забезпечують рамки для їх виконання.

Потенційно Україна може стати лідером у вивченні бізнес і кіберфінансових злочинів і боротьбі з ними, у неї може виникнути унікальна можливість створити глобальну нішу для своєї ІТ-індустрії і професіоналів, підвищити своє економічне зростання і зміцнити свою стратегічну безпеку.

У межах експериментального (пілотного) проєкту студентам УАУК і слухачам була запропонована навчальна програма «Основи корпоративної кібербезпеки», розрахована на 15 аудиторних навчальних занять, одне заняття – середньо-семестровий тест і одне заняття – фінальний тест. Загальний обсяг курсу: 3 американських кредити або 6 кредитів ЄКТС.

Проєктна версія онлайн курсу «Основи кібербезпеки підприємства» (для студентів УАКУ) наведена нижче у Додатку А (мовою оригіналу).

Курс «Основи корпоративної кібербезпеки» навчає компонентам успішного протистояння кіберзагрозам відповідно до програми кібербезпеки з точки зору людей, процесів і технологій. Орієнтуючись на людей, студент дізнається, як вирішувати проблеми кібербезпеки з точки зору бізнесу/місії. Студенти дізнаються, як працювати з технічними і бізнес-командами для вирішення критичних проблем кібергігієни. У процесі навчання студент дізнається, як розробляти політику, процедури, керівні принципи і стандарти, які будуть ефективними і підтримують місію їх організації.

Очікувані результати курсу. Після успішного завершення курсу студенти будуть мати необхідні знання і зможуть визначити наступні аспекти корпоративної кібербезпеки:

- ✓ Оцінити поточну ситуацію з безпекою, зокрема природу загрози, загальний стан загальних вразливостей і ймовірні наслідки збоїв безпеки.
- ✓ Критично оцінювати сильні і слабкі сторони загальних моделей кібербезпеки, у тріаді: конфіденційність – цілісність – доступність.
- ✓ Оцінити взаємозв'язки між елементами, що складають сучасну систему безпеки,

разом з апаратним забезпеченням, програмним забезпеченням, політикою і людьми.

- ✓ Оцінити, як взаємодіють всі галузі безпеки для досягнення ефективної загальносистемної безпеки на рівні підприємства.
- ✓ Порівняти взаємозв'язки між ролями та обов'язками в сфері безпеки в сучасному інформаційному підприємстві, щоб включити взаємозв'язки між доменами безпеки (IT, фізика, класифікація, персонал і т.д.).
- ✓ • Оцінити роль стратегії і політики у визначенні успіху інформаційної безпеки.
- ✓ • Оцінити можливі наслідки зсуву стратегії підприємства, політики і планів безпеки.
- ✓ Розробити концептуальний план інформаційної безпеки, який містить відповідні принципи управління життєвим циклом.
- ✓ Оцінити принципи ризику і провести концептуальне управління ризиками.
- ✓ Оцінити роль хороших метрик і ключових показників ефективності в оцінці безпеки та управлінні.
- ✓ Створити хороший набір показників інформаційної безпеки.
- ✓ Критика поточної нормативно-правового середовища щодо кібербезпеки.
- ✓ Виявити і зіставити найбільш поширені стандарти безпеки та відповідні каталоги заходів безпеки.
- ✓ Порівняти різні підходи до навчання безпеки і створення простої програми навчання.
- ✓ Обґрунтувати необхідність планування безперервності бізнесу і запропонувати, як успішно реалізувати такий план на сучасному підприємстві.
- ✓ Порівняти і зіставити логічну і фізичну безпеку.
- ✓ Оцінити поточну структуру ролей у галузі кібербезпеки в рамках умовного підприємства, разом з ролями і обов'язками відповідних організацій.
- ✓ Оцінити сильні та слабкі сторони сертифікації та акредитації підходів до кібербезпеки.
- ✓ Оцінити тенденції і моделі, які будуть визначати майбутній стан кібербезпеки.

Оцінюючи загалом результати реалізації експериментального (пілотного) проєкту дослідного навчання курсу основ корпоративної кібербезпеки студентів соціально-управлінського профілю, що не є профільними фахівцями в сфері інформаційно-комп'ютерних систем, інформаційного захисту та кібербезпеки, слід зазначити наступне:

1. Незважаючи на те, що навчання проводилось онлайн у несприятливих умовах широкого поширення COVID-19 і жорстких карантинних заходів, курс викликав інтерес як в українських, так і зарубіжних студентів 1-3 курсів спеціальності «бізнес-адміністрування» УАУК, а також слухачів з інших організацій.

2. Виявлено особливу зацікавленість більшої частини слухачів курсу, які брали активну участь у дискусіях і семінарах.

3. Деякі студенти з України та країн, що розвиваються, висловили адміністрації УАУК жаль, що не були обізнані з поняттями інформаційної та кіберзахисту в період їх шкільного навчання.

4. Під час викладання курсу проводились проміжкові тести, завершився курс оцінкою залишкових знань та виставленням фінальних оцінок.

5. Студенти, слухачі курсів і адміністрація УАУК мають намір додати до навчальних планів бакалаврських і магістерських програм навчання в УАУК (соціально-економічної, управлінської та міжнародної економічної спрямованості) спеціальні (елективні) курси з

інформаційного та кіберзахисту підприємства (корпоративний захист), фінансової, економічної і бізнес-адміністративної діяльності.

З каталогами УАУК з описом бакалаврських і магістерських програм 2019-2020 н.р. можна ознайомитись у[25] і [26], відповідно.

Усім громадянам України, які використовують або мобільний зв'язок, або комп'ютери з виходом в інтернет, або працюють з інформаційними мережами, слід знати основні інформаційні і кіберзагрози:

1. Типи загроз кібербезпеки.

Процес, пов'язаний з новими технологіями, тенденціями безпеки і аналізом загроз, є складним завданням. Однак це необхідно для захисту інформації та інших активів від кіберзагроз, які приймають різні форми. Кіберзагрози можуть включати в себе:

- ✓ Шкідливе ПЗ - це різновид шкідливого програмного забезпечення, при якому будь-який файл або програма може використовуватись для нанесення шкоди користувачеві комп'ютера, наприклад, черв'яки, комп'ютерні віруси, троянські програми і шпигунські програми.
- ✓ Атаки здирників – це тип шкідливих програм, при використанні яких зловмисник блокує комп'ютерні системні файли жертви – зазвичай за допомогою шифрування – і вимагає плату за розшифровку і розблокування.
- ✓ Соціальна інженерія – це атака, заснована на взаємодії людини з метою змусити користувачів порушувати процедури безпеки для отримання конфіденційної інформації, яка зазвичай захищена.
- ✓ Фішинг – це форма шахрайства, при якій відправляються шахрайські електронні листи, що нагадують електронні листи з надійних джерел; однак метою цих листів є крадіжка конфіденційних даних, таких як: дані кредитної картки або логін.

2. Елементи кібербезпеки.

Заходи з кібербезпеки забезпечують:

- ✓ Безпеку додатків.
- ✓ Інформаційну безпеку.
- ✓ Мережеву безпеку.
- ✓ Аварійне відновлення / планування безперервності бізнесу.
- ✓ Експлуатаційну безпеку.
- ✓ Навчання кінцевих користувачів.

3. Переваги кібербезпеки.

Переваги використання кібербезпеки включають в себе:

- ✓ Захист бізнесу від шкідливих програм, здирників, фішингу та соціальної інженерії.
- ✓ Захист даних і мереж.
- ✓ Запобігання неавторизованих користувачів.
- ✓ Зменшення часу відновлення після порушення.
- ✓ Захист для кінцевих користувачів.
- ✓ Підвищення довіри до продукту як для розробників, так і для клієнтів [27].

Також, з огляду на позитивний досвід вивчення в більшості середніх шкіл економічно розвинених країн таких предметів, як основи домашньої фінансової діяльності і просунуте навчання в сфері ІТ та інформаційної безпеки, було б доцільним ввести такі предмети, включаючи елементарні знання кіберзагроз та кібербезпеки, в навчальні плани в школах України.

Молодь України, як і інших пострадянських країн і держав постсоціалістичного табору, має перевагу перед молоддю демократичних, економічно розвинених країн. Вона

зумовлена соціально-економічною системою і історичним, культурним і повсякденним способом життя людей у цих країнах і більш коротким курсом середньої школи (у середньому на один рік менше, ніж у розвинених капіталістичних країнах), можливістю залишатися в сім'ї довше під наглядом батьків. Якщо в провідних демократичних країнах з ринковою економікою молоді люди віком 18-19 років, як правило, уже живуть окремо від батьків і заробляють собі на життя самостійно, то громадяни студентського віку, наприклад, України, мають кілька додаткових років, коли вони можуть продовжити навчання, перебуваючи під опікою сім'ї. Отже, в Україні існує ідеальна можливість більше вчитися і на практиці опанувати найперспективніші ІТ професії і стати конкурентоспроможними серед своїх однолітків з економічно розвинених країн. Про це свідчить лідируюча позиція України у відкритті стартапів.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведених досліджень і отриманого досвіду зроблено такі висновки:

1. Інформаційна і кібернетична безпека є пріоритетною для країн усього світу, особливо – для країн, що розвиваються, де захист від інтернет-злочинів поки не є достатньо ефективним.

2. Україна потребує інтенсивної освіти громадян усіх вікових груп з проблем фінансових злочинів і шахрайства з боку інтернет-хакерів і кіберзлочинців.

3. Поряд з професійним навчанням фахівців у сфері ІТ і кібербезпеки в Україні доцільно:

- ✓ ввести в школах навчання з питань захисту домашніх фінансів і домашніх (сімейних) господарств, основам ІТ і кібербезпеки;
- ✓ ввести в усіх професійних і закладах вищої освіти спеціальні дисципліни з навчання принципам, методам і технологіям ІТ і кіберзахисту фінансової, економічної та іншої професійної діяльності;
- ✓ організувати курсове навчання ІТ і кібербезпеки всіх зацікавлених громадян України.

4. В умовах послідовної Європейської інтеграції України необхідна тісна співпраця з організаціями та фахівцями з інформаційних технологій та кібербезпеки з економічно розвинених країн світу. Також доцільною є спільна із зарубіжними фахівцями розробка постійно оновлюваних наукових і інженерно-інформаційних технологій для протистояння викликам кіберзлочинності.

5. Підвищення рівня ІТ підготовки, обізнаності та спроможності українського населення орієнтуватись у кіберпросторі дозволить йому бути лідером в 4-й і 5-й промислової революції, зокрема в наступних трьох напрямах:

5.1. Цифрові розрахунки/криптовалюта. Відомо, що у великій частині світу швидко зросла популярність і цінність криптовалюти (біткойн, Ripple, Ethereum і т. д.). І, як і очікувалося, багато інвесторів втратили гроші. Недавня стабільність цін знову породила надію на те, що криптовалюти змінять стосунки між людьми і їх урядами, які мають одноосібне право випускати валюту.

Однак відомий американський інвестор і резидент Сінгапуру Джим Роджерс у своєму недавньому інтерв'ю розсудливо проаналізував майбутнє криптовалюти. «В уряду є те, чого немає у тих, хто працює з віртуальними валютами. Це зброя.» [28]. Якщо національні держави будуть гарантом вартості криптовалюти, то суспільство, добре

обізнане з використанням криптовалют, може отримати ринкову перевагу перед іншими суспільствами.

Існують країни з марними валютами, такі як Венесуела, що намагаються випустити цифрові валюти. Однак вони стикаються з тією ж нестачею довіри, що й до їх паперової валюти. Якщо український уряд зможе створити прозору цифрову валюту, яка буде прийнята кіберосвідомленим співтовариством, у нього буде унікальний сервіс і продукт, який шукають інші споживачі в світі: стабільна і офіційно прийнята криптовалюта, підтримувана економікою, досить великою, щоб відповідати будь-яким покупкам в його валюті.

Наприклад, причина, з якої долар США є найбільш часто використовуваною валютою, полягає в тому, що, якщо б у кого-небудь був один трильйон доларів США, він міг би легко придбати в Сполучених Штатах товари, власність і послуги на суму в один трильйон доларів США. Розмір має значення, тому євро і йена також є популярними засобами обміну. Україна, будучи великою і багатою ресурсами країною, може створити популярну криптовалюту.

5.2. Технологія ланцюжка блоків – Блокчейн, іноді званий технологією розподіленої книги (DLT - Distributed Ledger Technology), робить історію будь-якого цифрового активу незмінною і прозорою завдяки децентралізації та криптографічному хешуванню [29]. Як технології ланцюгових блоків можуть значно збільшити багатство України? Однією з основних перешкод на шляху розвитку на пострадянському просторі є недосконалі права власності і погана відстежуваність власності.

Великі багаті сільськогосподарські землі України не можуть бути належним чином оцінені і не можуть отримати доступ до капіталу і залучити інвестиції, тому що неможливо встановити і застрахувати право власності на них. Упровадження технології блокчейн для обліку власності призведе до швидкого зростання оцінки української економіки, стимулюючи роботу і ефективність її громадян і залучаючи капітал від інвесторів.

Децентралізована технологія ведення обліку, яка покликана прищепити довіру до справжності цифрових транзакцій, може бути використана для створення ефективних рішень як для комерційної, так і для житлової нерухомості – від купівлі нерухомості до проведення належної ретельності до надання можливості інвестуванню натовпу, і більше. Деякі великі компанії вже роблять ставку на техніку: гігант нерухомості RE/MAX уклав кілька партнерських угод для вивчення випадків використання блокчейну, тоді як Hilton Worldwide почала використовувати систему управління майном на основі блокчейна.

Блокчейн демонструє ефективність операцій з нерухомістю, підвищує потенціал зростання інвестицій і оцінок, а не тільки скорочення транзакційних витрат. На рис. 1 наведено порівняння поточних угод з нерухомістю та операцій з нерухомістю з ланцюжком блоків (купівля житла на Etherneum) [30].

Ethereum – криптовалюта і платформа для створення децентралізованих онлайн-сервісів на основі блокчейна, що працюють на базі розумних контрактів. Реалізована як єдина децентралізована віртуальна машина.

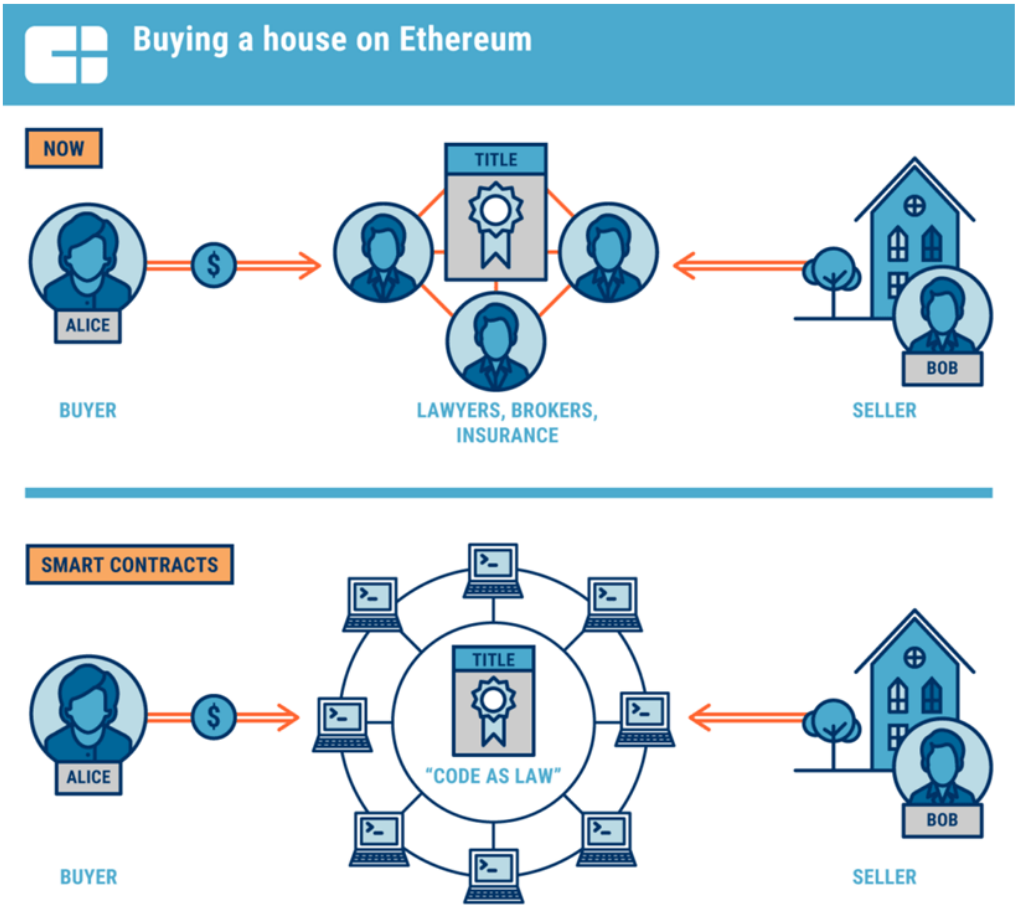

Рис. 1. Порівняння поточних угод з нерухомістю та операцій з нерухомістю з ланцюжком блоків (купівля житла на Etherneum)

Технологія блокчейн пропонує форму спільного ведення записів, розроблену так, що її важко підробити. Технологія блокчейн працює за допомогою децентралізованих однорангових платформ, забезпечуючи стійкість до поширення пошкодженої інформації та підвищуючи опір шахрайству.

Технологія блокчейн має потенціал для вирішення багатьох проблем у галузі нерухомості, зокрема:

- ✓ Поліпшення довіри та прозорості: Технологія блокчейн пропонує перевірений та стійкий до цензури варіант для обміну інформацією (наприклад, деталями оцінки).
- ✓ Скорочення відібраних баз даних: процеси нерухомості отримали б користь від захищених від несанкціонованих спільних баз даних, які збирають дані та документи різних зацікавлених сторін в одному місці.
- ✓ Підвищення ефективності процесів транзакцій: більшість операцій з нерухомістю все ще проводяться за допомогою банківських переказів і вимагають дорогих процесів перевірки, які можуть зайняти кілька днів. Блокчейн на основі транзакцій може забезпечити спрощений процес, який забезпечує швидкість та зменшує витрати.
- ✓ Обмеження використання посередників: багато посередників – від брокерів до

ескроу-компаній – можуть бути застарілими шляхом підходів, заснованих на блокчейн, оскільки записи можна зберігати, перевіряти та передавати за допомогою технології блокчейн. Усунення потреби в посередниках може значно зменшити витрати та заощадити час.

Ескроу-компанія – це компанія, що користується депозитним правом, зазвичай використовується в операціях з нерухомістю, зберігає гроші та документи сторін. Будучи нейтральною третьою стороною, компанія з депозитування допомагає полегшити процес купівлі та продажу дому.

На рис. 2 схематично показано, як працює технологія блокчейн [30].

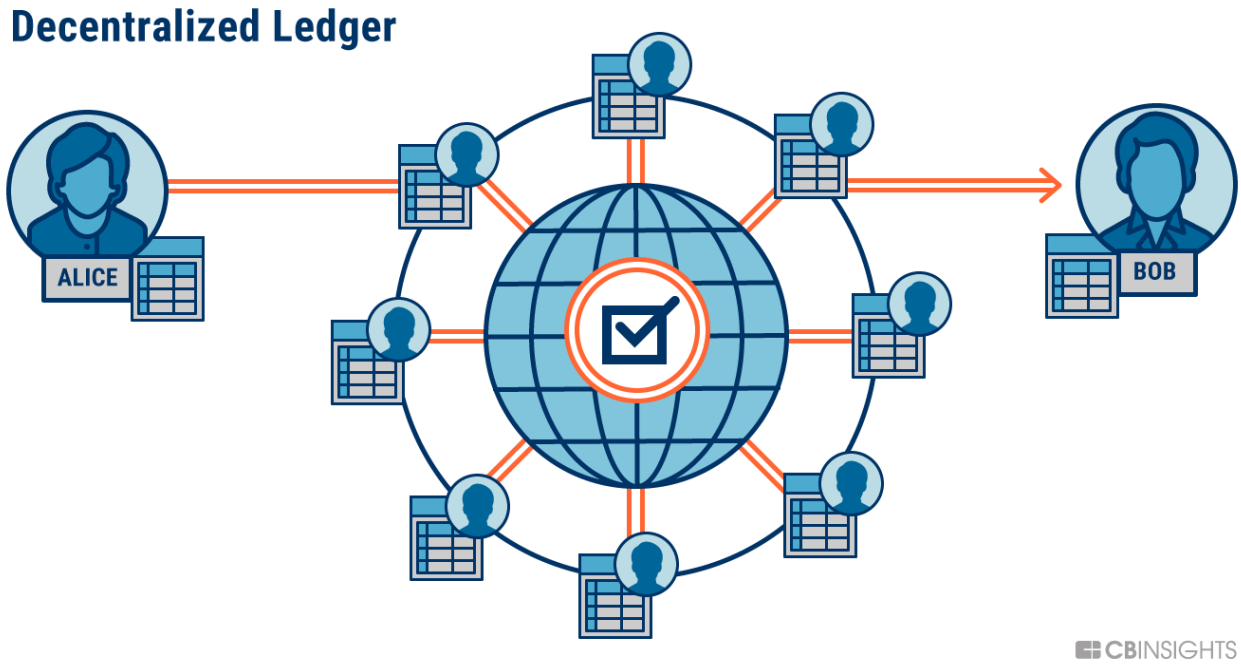

Рис. 2. Схематичне зображення роботи технологія блокчейн

5.3. 3D-друк. Оскільки пандемія COVID-19 і геополітична напруженість порушують світові ланцюжки поставок, країни, які можуть налагодити власне внутрішнє виробництво простих у виробництві компонентів, матимуть конкурентну перевагу в продажу своєї кінцевої продукції і послуг на світовому ринку. Прикладом конкурентної переваги низької ціни на природний газ в Сполучених Штатах є низька цінова складова у виробничих витратах на його видобуток.

Крім того, стабільне внутрішнє виробництво компонентів додасть економікам цих країн стійкості до коливань пропозиції, які в даний час спостерігаються під час пандемії COVID. Оскільки виробники і продавці в Європі і США не змогли отримати базові компоненти, у результаті їм довелося звільняти свою робочу силу.

Згідно з останніми даними, до COVID обсяг 3D-друку збільшувався на 24% в рік, подвоюючись кожні 3 роки [31]. Однак ми повинні очікувати, що інвестори будуть прискорювати зростання. Україна має унікальний потенціал, щоб скористатися цими інвестиціями і можливостями попиту. Нижче наведено рис.3, узятий зі звіту початку 2020

року про очікуване зростання 3D-друку [32].

Рис. 3. Прогнозоване зростання вартості 3D-друку (в млрд. доларів США)

Українське населення, ознайомлене, навчене і здатне працювати в цих нових сферах інформаційних технологій, може сприяти підвищенню рівня життя своїх громадян, а також загального добробуту і продуктивності нації. Методична і старанна підготовка учнів, студентів і фахівців стане підґрунтям для зростання добробуту і благополуччя нашої країни.

ДОДАТОК А

Experimental version
"Essentials of Enterprise Cyber Security"
Syllabus (for on-line course)
Spring 2020

Quarter/Year: Spring /2020
ECTS Credits: 6
US Credits: 3
Consultation hours: By appointment

Prerequisites: None
Course Description
The course, Essentials of Enterprise Cyber Security, will teach the components of a successful cyber security program from a people, process, and technology perspective. Focusing on people, the student will learn how to address cyber security challenges from a business / mission perspective. Students will learn how to work with technical and business teams to address critical cyber hygiene issues. When addressing process, the student will learn how to develop policies, procedures, guidelines, and standards that are effective and support their organization's mission.

Course Outcomes
Upon successful completion of this course, students will be **familiar and able to define** the following aspects of Enterprise Cyber Security:

- ✓ Assess the current security landscape, including the nature of the threat, the general status of common vulnerabilities, and the likely consequences of security failures
- ✓ Critique and assess the strengths and weaknesses of general cybersecurity models, including the CIA triad
- ✓ Appraise the interrelationships among elements that comprise a modern security system, including hardware, software, policies, and people
- ✓ Assess how all domains of security interact to achieve effective system-wide security at the enterprise level.
- ✓ Compare the interrelationships among security roles and responsibilities in a modern information-driven enterprise—to include interrelationships across security domains (IT, physical, classification, personnel, and so on)
- ✓ Assess the role of strategy and policy in determining the success of information security
- ✓ Estimate the possible consequences of misaligning enterprise strategy, security policy, and security plans
- ✓ Design a notional information security plan that incorporates relevant principles of lifecycle management
- ✓ Evaluate the principles of risk and conduct a notional risk management exercise
- ✓ Assess the role of good metrics and key performance indicators (KPIs) in security assessment and governance
- ✓ Create a good set of information security metrics
- ✓ Critique the current legal and regulatory environment as it applies to cybersecurity
- ✓ Identify and contrast the most common security standards and associated catalogues of security controls
- ✓ Contrast the various approaches to security training and formulate a simple training agenda

- ✓ Justify the need for business continuity planning and propose how to implement such a plan successfully within a modern enterprise
- ✓ Compare and contrast logical and physical security
- ✓ Appraise the current structure of cybersecurity roles across a notional enterprise, including the roles and responsibilities of the relevant organizations
- ✓ Assess the strengths and weaknesses of the certification and accreditation approach to cybersecurity
- ✓ Evaluate the trends and patterns that will determine the future state of cybersecurity

Internationality: International textbooks and software tools

Communications

For individual issues, students should contact the professor ONLY by given e-mail or by Moodle. In the Subject line they should put: **UACUFirstNameLastName**. E-mail messages will normally be answered within 24 hours.

Student Responsibilities

Time Commitment

The study of technical courses is cumulative (i.e., an understanding of earlier material is necessary to grasp concepts covered later). Past experience has shown a high correlation between procrastination and low grades. Students must be committed to completing tasks on time.

Grading Policy

The course is based on mastery of course outcomes. The student's grade for this course will be calculated based on performance.

Note: the minimal grade to pass a subject is **60% (for Bachelor's degree). 70% (for Master's degree).**

Graduate Grading Guidelines

The assignment of a letter grade for a course is an indication of the student's overall success in achieving the learning outcomes for the course. The course letter grade may be viewed as a summary statement of the student's achievement in individual assessments (assignments & activities). These assessments are intended to identify for students their strengths as well as those areas in need of improvement. Student work is assessed according to the guidelines below.

Course-level Grading guidelines:

Grade	ECTS Grade	International Grade
90% - 100%	**A**	**5 (Excellent)**
83% - 89%	**B**	**4 (Very Good)**
75% - 82%	**C**	**4 (Good)**
70% - 74%	**D**	**3 (Good)**
60% - 69%	**E**	**3 (Acceptable)**
35% - 59%	**FX**	**Not acceptable, possible repetition of course**

Criteria for grading:

ECTS grade	Requirements for the student
A	The student demonstrated a comprehensive systemic and in-depth knowledge of program material; processed basic and additional literature; obtained a solid grasp of the conceptual apparatus, methods, techniques and tools provided by the program; found creative abilities in the presentation of the educational program material both on this issue and on related modules of the course and related courses, or the student had a current control of 90-100 points
B	The student demonstrated good knowledge of program material; processed the basic literature, mastered the conceptual apparatus, methods, techniques and tools provided by the program, but with some inaccuracies
C	
D	The student showed mediocre knowledge of the core program material; learned information mainly from a lecture course or just one textbook; mastered only certain methods, techniques and tools provided by the program
E	
FX	The student has significant gaps in knowledge of the main program material; fragmentary mastered the basic concepts, techniques and tools; significant mistakes are made when using them

Undergraduate Students: Maximum total possible points – **225** points incl. (midterm and final exam are **60%** of overall evaluation, where Midterm – **20%** and Final – **40%**)

- ✓ Class participation (via online discussion) / Test / Assignment **–3/3**points (every week / several times during the course)- **90** points (40%)
- ✓ Midterm exam**- 45** points (20%)
- ✓ Final exam **– 90** points (40%)

Graduate Students: The following provides an approximate breakdown of how each assignment contributes to the overall performance in the class.

- Class participation (via online discussion) /Test / Assignment **–1.5/1.5** points (every week / several times during the course)- **45** points (20%)
- Midterm exam**- 22.5** points (10%)
- Final exam **– 45** points (20%)
- Research paper – **67.5** points (30%)
- Security Project – **45** points (20%)

Research Paper (30%):

The students will be required to write a graduate-level research paper (10 pages, double spaced, not including front matter and bibliography). The paper will allow the students to delve more deeply into the challenges of managing the systems that help assure the confidentiality, integrity, and availability of information. Outside research will be required.

Students will deliver the paper in three phases: (1) an annotated bibliography of sources, (2) a draft of the completed paper, and (3) a final version of the paper. This phased approach will allow the instructor to provide students with feedback along the way instead of only at the end of the project. Overall, the students will be required to evaluate the topic with an eye toward defending and justifying a well-reasoned position.

Security Project (20%):

In the security project, each student will prepare a notional security plan and notional risk

assessment (approximately 10 pages, double spaced, not including the risk assessment spreadsheet). This plan will address the issues discussed in the texts and the course and tailor the plan to a context defined by the student. This risk assessment will be built using MITRE's Risk Matrix tool, and NIST Framework. It will reflect real-world conditions but not represent a real-world system or enterprise. The student will be expected to apply a superior level of analysis when creating the combined plan.

Assignment Format

- ✓ **All work should be shown in time. If the student misses the deadline – the task is failed**
- ✓ **Assignments (projects) should be done in Word MS/PPT, contain an introduction, main part, conclusions, and references. The volume up to 10 pages/ 10 slides**
- ✓ **Midterm covered topics from previous lectures (weeks 1-6). It included multiple choice questions and cases (essays) and took about 1 hour.**
- ✓ **The final exam covered all course material and included multiple choice questions and cases (essays). It longs for 1,5 hours. Admission to the final exam is possible only if all the tasks of the curriculum are covered**

Academic dishonesty

1. Academic integrity is submitting one's own work and properly acknowledging the contributions of others. Any violation of this principle constitutes academic dishonesty and is liable to result in a failing grade and disciplinary action. Forms of academic dishonesty include:
   - **Plagiarism** — submitting all or part of another's work as one's own in an academic exercise such as an examination, a computer program, or written assignment.
   - **Cheating** — using or attempting to use unauthorized materials on an examination or assignment, such as using unauthorized texts or notes or improperly obtaining (or attempting to obtain) copies of an examination or answers to an examination.
   - **Facilitating Academic Dishonesty** — helping another commit an act of dishonesty, such as substituting for an examination or completing an assignment for someone else.
   - **Fabrication** — altering or transmitting, without authorization, academic information or records.
2. **Midterm and Final are valid only if they are taken on-campus (room defined by the dean's office) and on UACU's computer/laptop. Students who will not meet this requirement will be expelled from the course with grade "0".**
3. **In case of missed midterm or final exam (for a valid reason like sickness or an emergency) a request to repeat the exam is possible. Permit to repeat a midterm or final exam is done through a letter to the dean's office with request and approval of subject lecturer.**
4. **Submission or retaken of any assessment activities after deadlines are forbidden.**
5. **Submission & Return Policy**

Assignments must be submitted to the professor on or before the due date indicated in the Course Schedule. The assignments submitted after the due dates receive zero points.

****** NO MAKE–UP QUIZZES AND EXAMS ******

Schedule

Week #	Topics	Method of instruction	Assignments Due	Points (Under-Graduate)
Week 1	**The Security Environment** – Threats, vulnerabilities, and consequences – Advanced persistent threats – The state of security today – Why security matters to commercial enterprises	**Lecture** **-** **Online Discussion**	**Student Introduction**	**3/3**
Week 2	**Principles of Cybersecurity** – The interrelated components of the computing environment – Cybersecurity models (the CIA triad, the star model, the Parkerian hexad) – Variations on a theme: computer security, information security, and information assurance	**- Pre-reading** **- Lecture** **- Online Discussions**	**Review Lecture** **Test / Assignment**	**3/3**
Week 3	**Cybersecurity Management Concepts** – Security governance – Management models, roles, and functions	**- Pre-reading** **- Lecture** **- Online Discussions**	**Review Lecture** **Test / Assignment**	**3/3**
Week 4	**Enterprise Roles and Structures** – Information security roles and positions – Alternative enterprise structures and interfaces	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment** **Annotated bibliography (Graduate Students)**	**3/3**
Week 5	**Strategy and Strategic Planning** – Strategy – Strategic planning and security strategy – The information security lifecycle – Architecting the enterprise	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment**	**3/3**
Week 6	**Security Plans and Policies** – Levels of planning – Planning misalignment – The System Security Plan (SSP) – **Policy development and implementation** Laws and Regulatory Requirement – Timeline of international laws related to information security – EU and US regulations	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment**	**3/3**
Week 7	**Midterm Exam**	- Pre-reading - Lecture - Online Discussions	Review Lecture Test / Assignment	***45***

Week 8	Security Standards and Controls – Security standards and controls – Certification and accreditation (C&A)	- Pre-reading - Lecture - Online Discussions	Review Lecture Test / Assignment **Research paper (draft) (Graduate Students)**	**3/3**
Week 9	Risk Management – Principles of risk – Types of risk – Risk strategies – The Risk Management Framework (RMF)	- Pre-reading - Lecture - Online Discussions	**Review Lecture** Test / Assignment	**3/3**
Week 10	**Security Metrics and Key Performance Indicators (KPIs)** – The challenge of security metrics – What makes a good metric – Approaches to security metrics – Metrics and Regulation	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment** **Research paper (final version) (Graduate Students)**	**3/3**
Week 11	**Physical Security and Environmental Events** – Physical and environmental threats – Physical and environmental controls	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment**	**3/3**
Week 12	**Contingency Planning** – Developing a contingency plan – Understanding the different types of contingency plan – Responding to events	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment**	**3/3**
Week 13	**Security Education, Training, and Awareness** – Human factors in security – Developing and implementing a security training plan – Cross-domain training (IT and other security domains)	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment**	**3/3**
Week 14	**Managing information security across a commercial enterprise (1)** – The purpose of certification and accreditation – Trends in certification and accreditation	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment** **Security Project (Graduate Students)**	**3/3**
Week 15	**Managing information security across a commercial enterprise (2)** – The strategic direction of enterprise IT and information security – Responsibilities within the commercial enterprise	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment**	**3/3**

Week 16	**The future of cybersecurity** – Key future uncertainties – Possible future scenarios – How to apply what you've learned	- Pre-reading - Lecture - Online Discussions	**Review Lecture** **Test / Assignment**	**3/3**
Week 17	**Final Exam**			**90**
				225

Recommended Materials

There are no textbook requirements for the course. The instructor will provide readings, videos, podcasts, and notes from the following sources under the Fair Use Copyright Act (see https://www.copyright.gov/fair-use/more-info.html)

(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide 8th Edition, Kindle Edition by Mike Chapple (Author), James Michael Stewart (Author), Darril Gibson (Author) Microsoft Access 2013 Part 2
Information Security: The Complete Reference, Second Edition 2nd Edition, by Mark Rhodes-Ousley (Author)

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Jessica Lindsay and Alex Hudson. "What is the fifth industrial revolution and how will it change the world?" [Електронний ресурс]. Доступно: https://metro.co.uk/2019/06/10/fifth-industrial-revolution-will-change-world-9738825/. Дата звернення: 15.04.2020

[2] The fifth industrial revolution. When humans and machines combine. *Digital Technology*, Apr.03, 2018. [Електронний ресурс]. Доступно: https://www.genpact.com/insight/blog/the-fifth-industrial-revolution. Дата звернення: 15.04.2020

[3] Stuart Lauchlan, "The Fifth Industrial Revolution is coming – and it's about trust, values and saving the planet". [Електронний ресурс]. Доступно: https://diginomica.com/the-fifth-industrial-revolution-is-coming-and-its-about-trust-values-and-saving-the-planet. Дата звернення: 15.04.2020

[4] Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond". [Електронний ресурс]. Доступно: https://www.weforum.org/agenda/authors/klaus-schwab. Дата звернення: 15.04.2020

[5] Deep Shift Technology Tipping Points and Societal Impact. WORLD ECONOMIC FORUM, 2015. [Електронний ресурс]. Доступно: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[6] Закон № 2163-VIII "Про основні засади забезпечення кібербезпеки України" (Відомості Верховної Ради), № 45, с. 403, 2017.

[7] Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. Національний інститут стратегічних досліджень. [Електронний ресурс]. Доступно: http://old2.niss.gov.ua/articles/294/. Дата звернення: 10.02.2020.

[8] 2019 Internet Crime Report. [Електронний ресурс]. Доступно: https://pdf.ic3.gov/2019_IC3Report.pdf. Дата звернення: 11.05.2020

[9] S. LaBello, "The Biggest Cyber Threats in 2019". [Електронний ресурс]. Доступно: https://www.pratum.com/blog/429-the-biggest-cyber-threats-in-2019. Дата звернення: 12.05.2020

[10] R. McLean, "A hacker gained access to 100 million Capital One credit card applications and accounts", *CNN Business,* July 30, 2019. [Електронний ресурс]. Доступно: https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html. Дата звернення: 04.03.2020

[11] D. Barrett, "Capital One says data breach affected 100 million credit card applications", *The Washington Post,* July 30, 2019. [Електронний ресурс]. Доступно: https://www.washingtonpost.com/national-security/capital-one-data-breach-compromises-tens-of-millions-of-credit-card-applications-fbi-says/2019/07/29/72114cc2-b243-11e9-8f6c-7828e68cb15f_story.html. Дата звернення: 05.03.2020

[12] Cybersecurity Industry Associations. *Cyber Crime Magazine.* [Електронний ресурс]. Доступно: https://cybersecurityventures.com/cybersecurity-associations/. Дата звернення: 25.05.2020
[13] WORLD BANK GROUP. Financial Sector's Cybersecurity: A Regulatory Digest∗. 2019 World Bank's FinSAC Digest of Cybersecurity Regulations in the Financial Sector, 113 p. [Електронний ресурс]. Доступно: http://pubdocs.worldbank.org/en/940481575300835196/CybersecDIGEST-NOV2019-FINAL.pdf. Дата звернення: 05.04.2020
[14] WORLD BANK GROUP. Global Cybersecurity Capacity Program. Lessons Learned and Recommendations towards strengthening the Program. 2019 The World Bank, 68 p. [Електронний ресурс]. Доступно: http://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf. Дата звернення: 10.04.2020
[15] Защита денег: на борьбу с киберугрозами банки тратят больше, чем на развитие отделений. [Електронний ресурс]. Доступно: https://delo.ua/econonomyandpoliticsinukraine/dorogaja-zaschita-na-borbu-s-kiberugrozami-banki-363177/. Дата звернення: 10.02.2020.
[16] Больше всего от кибератак страдает малый и средний бизнес – исследование. [Електронний ресурс]. Доступно: https://delo.ua/business/bolshe-vsego-ot-kiberatak-stradaet-malyj-i-sredn-360727/ . Дата звернення: 10.02.2020.
[17] Фишинг: Как не попасться на удочку. [Електронний ресурс]. Доступно: https://delo.ua/business/fishing-kak-ne-popastsja-na-udochku-357348/. Дата звернення: 10.02.2020.
[18] D.Schatz, R.Bashroush and Ju. Wall, "Towards a More Representative Definition of Cyber Security", *Journal of Digital Forensics, Security and Law*, 12(2), Article 8, 53-74, 2017. [Електронний ресурс]. Доступно: https://commons.erau.edu/jdfsl/vol12/iss2/8/
[19] В.Ю.Биков, О.Ю.Буров та Н.П.Дементієвська, «Кібербезпека в цифровому навчальному середовищі», *Інформаційні технології та засоби навчання* , 2(70), 313–331, 2019.
[20] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, "Guidelines for Smart Grid Cybersecurity", NISTIR 7628 Rev. 1. [Електронний ресурс]. Доступно:
https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final. Дата звернення: 04.03.2020
[21] ITU-T X.1205, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security, Overview of cybersecurity. International Telecommunication Union, 64 p. [Електронний ресурс]. Доступно: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=en. Дата звернення: 04.03.2020
[22] Tari Schreider, "Cybersecurity Law, Standards and Regulations, 2nd Edition", Rothstein Publishing; February 2020 [Електронний ресурс]. Доступно: https://www.ebooks.com/en-ua/book/209962921/cybersecurity-law-standards-and-regulations-2nd-edition/schreider-tari/?src=feed&gclid=CjwKCAjwyo36BRAXEiwA24CwGXnZH2wh9MpES6XqZ1aTj7qPkIBoX2douv55V34EXIxH8oRpwj3CpBoC1mAQAvD_BwE. Дата звернення: 29.06.2020
[23] PriceWaterhouseCooper (PwC). "Global Economic Crime and Fraud Survey 2018: Ukrainian findings Pulling fraud out of the shadows". [Електронний ресурс]. Доступно:
https://www.pwc.com/ua/en/survey/2018/pwc-gecs-2018-eng.pdf Дата звернення: 13.04.2020
[24]J. Clement, "IC3: total damage caused by reported cyber crime 2001-2019". In: Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2019 (in million U.S. dollars). [Електронний ресурс]. Доступно: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/#statisticContainer . Дата звернення: 15.04.2020
[25] Ukrainian-American University Bachelor Programs Catalog 2019-2020. [Електронний ресурс]. Доступно: https://www.concordia.edu.ua/wp-content/uploads/2020/02/2020-bba-catalog.pdf. Дата звернення: 02.03.2020
[26] Ukrainian-American University Master's Degree Programs Catalog 2019-2020. [Електронний ресурс]. Доступно: https://www.concordia.edu.ua/wp-content/uploads/2019/07/ConcordiaUA-MBA-Catalog-Updated.pdf. Дата звернення: 02.03.2020
[27] M. Rouse, "What is Cybersecurity? Everything You Need to Know". [Електронний ресурс]. Доступно: https://searchsecurity.techtarget.com/definition/cybersecurity. Дата звернення: 25.05.2020
[28] Kevin Helms, "Jim Rogers Discusses Bitcoin as Money and Why Governments Will Stop Crypto" [Електронний ресурс]. Доступно:https://news.bitcoin.com/jim-rogers-bitcoin/. Дата звернення: 21.07.2020
[29] BuiltIn Journal, "Blockchain. What Is Blockchain Technology? How Does Blockchain Work?
[Електронний ресурс]. Доступно: https://builtin.com/blockchain. Дата звернення: 21.07.2020
[30] CBInsights, "How Blockchain Technology Could Disrupt Real Estate". [Електронний ресурс]. Доступно:

https://www.cbinsights.com/research/blockchain-real-estate-disruption/. Дата звернення: 21.07.2020
[31] Tia Vialva, "3D Hubs 3D Printing Trends Report Forecasts 24% Growth in 3D Printing Industry over 5 Years". [Електронний ресурс]. Доступно: https://3dprintingindustry.com/news/3d-hubs-3dprinting-trends-report-forecasts-24-growth-in-3d-printing-industry-over-5-years-167998/. Дата звернення: 21.07.2020
[32] Statista Research Department, May 11, 2020 "3D printing industry - worldwide market size 2020-2024" . [Електронний ресурс]. Доступно: https://www.statista.com/statistics/315386/global-market-for-3dprinters/. Дата звернення: 21.07.2020

Матеріал надійшов до редакції __.__.201_ р.

ОБУЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ И КИБЕРЗАЩИТЕ СПЕЦИАЛИСТОВ ПО УПРАВЛЕНИЮ ФИНАНСАМИ, ЭКОНОМИКОЙ И БИЗНЕСОМ

Быков Валерий Ефимович
доктор технических наук, профессор, академик НАПН Украины, директор
Институт информационных технологий и средств обучения НАПН Украины, г. Киев, Украина
ORCID ID 0000-0002-5890-6783
valbykov@gmail.com

Романовский Александр Алексеевич
доктор педагогических наук, доктор экономических наук, профессор, ректор
Украинско-американский университет Конкордия, г. Киев, Украина
ORCID ID 0000-0002-3618-2999
oleksandr.romanovskyi@uacu.edu.ua

Романовская Юлия Юрьевна
кандидат филологических наук, профессор, вице-ректор
Украинско-американский университет Конкордия, г. Киев, Украина
ORCID ID 0000-0002-0207-3348
yuliia.romanovska@uacu.edu.ua

Аннотация. Исследование посвящено необычно актуальной теме повышения киберграмотности населения. Исследование базируется на уникальном опыте межнационального учебного проекта «Основы корпоративной кибербезопасности». Цель данной работы – предложить подход к решению проблемы подготовки граждан Украины (и, возможно, граждан других стран) к противодействию киберугрозам в их профессиональной деятельности. Объектом исследования является финансовая индустрия, которая является частью программ старших классов/курсов колледжей и университетов во многих странах. Авторы выдвигают такую идею: научить основам кибербезопасности неспециалистов в сфере ИТ – тех, кто не имеет специальной инженерно-технической подготовки в области ИТ и киберзащиты, и специалистов в сфере социальной защиты – экономическая сфера (бизнес-лидеры, предприниматели, экономисты, финансисты и др.) – необходимо учить их кибербезопасности, ориентированной на их профессиональную деятельность. В результате проведенных исследований авторами определено, что во многих странах, особенно в развивающихся, киберпреступность является серьезной проблемой. Авторы подтверждают, что Украине необходимо интенсивное обучение граждан всех возрастов проблемам финансовых преступлений и мошенничества со стороны интернет-хакеров и киберпреступников. Наряду с профессиональной подготовкой специалистов в области информационных технологий и кибербезопасности, в Украине целесообразно: ввести в школьную систему обучение по домашним финансам и методам их ИТ защиты; ввести обучение основам информационных технологий, кибербезопасности, финансов и экономики во всех колледжах, институтах и университетах; организовать обучение в сфере информационных технологий и кибербезопасности для граждан Украины. Для обеспечения интеграции Украины с Европой необходимо тесное сотрудничество с развитыми странами и транснациональными организациями для развития процветающего сектора кибербезопасности. В Украине достаточно грамотных молодых специалистов в области ИТ, которые успешно работают на зарубежные

компании и корпорации. Необходимо эффективно использовать этот человеческий ресурс и целесообразно создать координирующий обучающий центр по кибербезопасности в области экономической и финансовой деятельности.

Ключевые слова: киберугроза; кибератака; кибермошенничество; киберзащита бизнеса и финансов; обучение корпоративной финансовой кибербезопасности.

TRAINING OF CYBER SECURITY AND CYBER DEFENSE FOR SPECIALISTS OF FINANCE, ECONOMIC AND BUSINESS MANAGEMENT

Valeriy Yu. Bykov
Doctor of Technical Sciences, Professor, Academician of NAES of Ukraine, Director
Institute of Information Technologies and Learning Tools of NAES of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-5890-6783
valbykov@gmail.com

Alexander A. Romanovsky
Doctor of Education, Doctor of Economics, Professor, Rector
Ukrainian-American University Concordia, Kiev, Ukraine
ORCID ID 0000-0002-3618-2999
oleksandr.romanovskyi@uacu.edu.ua

Julia Yu. Romanovskaya
Candidate of Philological Sciences, Professor, Vice Rector
Ukrainian-American University Concordia, Kiev, Ukraine
ORCID ID 0000-0002-0207-3348
yuliia.romanovska@uacu.edu.ua

Abstract. The study is devoted to the extremely relevant topic - increasing population cyber awareness and based on the unique experience of the transnational training project "Fundamentals of Corporate Cybersecurity". The aim of this work is to offer a partial solution to the problem of preparing Ukrainian citizens (and potentially citizens from other countries) to confront cyber threats in their professional activities. The object of the study is the finance industry, which is a part of the high school programs of colleges and universities in many countries. The authors put forward the idea that: to prepare of non-specialists in the IT field on the basics of cyber protection - those who do not have special engineering and technical training in the field of IT and cyber defense, and specialists in the socio-economic sphere (business leaders, entrepreneurs, economists, financiers and others) - it is necessary to train on cybersecurity, which is focused on their professional activities.

As a result of the studies, the authors concluded, that in many countries, especially developing countries, cybercrime is a major problem. The authors prove, that Ukraine needs intensive education of citizens of all age groups on the problems of financial crimes and fraud by Internet hackers and cyber criminals. Along with the professional training of specialists in the field of IT and cybersecurity, in Ukraine it is advisable to: Introduce education on home finance and technologies for their IT protection in the school system; to prepare of non-specialists in the IT field on the basics of cyber protection on the principles of IT, cybersecurity, financial, and economics in all of colleges, institutions and universities; organize training in IT and cybersecurity for Ukrainian citizens. To ensure Ukraine's integration with Europe, close cooperation with developed nations and transnational organizations is crucial to developing a thriving cybersecurity sector. Ukraine has competent young IT specialists who successfully work for foreign companies and corporations. It is necessary to effectively use this human resource and it is advisable to create a coordinating training center for cybersecurity in the field of economic and financial activities.

Keywords: cyber threat; cyberattack; cyber fraud; cyber defense of business and finance; corporate financial cybersecurity training.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Jessica Lindsay and Alex Hudson. "What is the fifth industrial revolution and how will it change the world?" [Online]. Avalible: https://metro.co.uk/2019/06/10/fifth-industrial-revolution-will-change-world-9738825/. Accessed on: 15.04.2020 (in English)

[2] The fifth industrial revolution. When humans and machines combine. *Digital Technology*, Apr.03, 2018. [Online]. Available: https://www.genpact.com/insight/blog/the-fifth-industrial-revolution. Accessed on: 15.04.2020 (in English)

[3] Stuart Lauchlan, "The Fifth Industrial Revolution is coming – and it's about trust, values and saving the planet." [Online]. Available: https://diginomica.com/the-fifth-industrial-revolution-is-coming-and-its-about-trust-values-and-saving-the-planet. Accessed on: 15.04.2020 (in English)

[4] Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond." [Online]. Available: https://www.weforum.org/agenda/authors/klaus-schwab. Accessed on: 15.04.2020 (in English)

[5] Deep Shift Technology Tipping Points and Societal Impact. WORLD ECONOMIC FORUM, 2015. [Online]. Available: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf (in English)

[6] Law № 2163-VIII "About the basic principles of providing cyber security of Ukraine." (Vidomosti Verkhovnoi Rady), no. 45, p. 403, 2017 (in Ukrainian)

[7] Current trends in cybersecurity policy: conclusions for Ukraine. Analytical note. National Institute for Strategic Studies. [Online]. Available: http://old2.niss.gov.ua/articles/294/. Accessed on: 10.02.2020 (in Ukrainian)

[8] 2019 Internet Crime Report. [Online]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf. Accessed on: 11.05.2020 (in English)

[9] S. LaBello, "The Biggest Cyber Threats in 2019." [Online]. Available: https://www.pratum.com/blog/429-the-biggest-cyber-threats-in-2019. Accessed on: 12.05.2020 (in English)

[10] R. McLean, "A hacker gained access to 100 million Capital One credit card applications and accounts," *CNN Business,* July 30, 2019. [Online]. Available: https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html. Accessed on: 04.03.2020 (in English)

[11] D. Barrett, "Capital One says data breach affected 100 million credit card applications," *The Washington Post,* July 30, 2019. [Online]. Available: https://www.washingtonpost.com/national-security/capital-one-data-breach-compromises-tens-of-millions-of-credit-card-applications-fbi-says/2019/07/29/72114cc2-b243-11e9-8f6c-7828e68cb15f_story.html. Accessed on: 05.03.2020 (in English)

[12] Cybersecurity Industry Associations. *Cyber Crime Magazine.* [Online]. Available: https://cybersecurityventures.com/cybersecurity-associations/. Accessed on: 25.05.2020 (in English)

[13] WORLD BANK GROUP. Financial Sector's Cybersecurity: A Regulatory Digest∗. 2019 World Bank's FinSAC Digest of Cybersecurity Regulations in the Financial Sector, 113 p. [Online]. Available: http://pubdocs.worldbank.org/en/940481575300835196/CybersecDIGEST-NOV2019-FINAL.pdf. Accessed on: 05.04.2020 (in English)

[14] WORLD BANK GROUP. Global Cybersecurity Capacity Program. Lessons Learned and Recommendations towards strengthening the Program. 2019 The World Bank, 68 p. [Online]. Available: http://documents1.worldbank.org/curated/en/947551561459590661/pdf/Global-Cybersecurity-Capacity-Program-Lessons-Learned-and-Recommendations-towards-Strengthening-the-Program.pdf. Accessed on: 10.04.2020 (in English)

[15] Money protection: banks spend more on cyber threats than on branch development. [Online]. Available: https://delo.ua/econonomyandpoliticsinukraine/dorogaja-zaschita-na-borbu-s-kiberugrozami-banki-363177/. Accessed on: 10.02.2020 (In Russian)

[16] Small and medium-sized businesses suffer the most from cyberattacks – research. [Online]. Available: https://delo.ua/business/bolshe-vsego-ot-kiberatak-stradaet-malyj-i-sredn-360727/. Accessed on: 10.02.2020 (in Russian)

[17] Phishing: How not to fall for the bait. [Online]. Available: https://delo.ua/business/fishing-kak-ne-popastsja-na-udochku-357348/. Accessed on: 10.02.2020 (in Russian)

[18] D.Schatz, R.Bashroush and Ju. Wall, "Towards a More Representative Definition of Cyber Security," *Journal of Digital Forensics, Security and Law*, 12(2), Article 8, 53-74, 2017. [Online]. Available: https://commons.erau.edu/jdfsl/vol12/iss2/8/ (in English)

[19] V. Yu. Bykov, O. Ju. Burov, N. P. Dementievska, "Cyber Security in a Digital Learning Environment," *Information Technologies and Learning Tools*, 70(2), pp. 313–331, 2019. (in Ukrainian)

[20] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, "Guidelines for Smart Grid

Cybersecurity," NISTIR 7628 Rev. 1. [Online]. Available:
https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final. Accessed on: 04.03.2020 (in English)
[21] ITU-T X.1205, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security, Overview of cybersecurity. International Telecommunication Union, 64 p. [Online]. Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=en. Accessed on: 04.03.2020 (in English)
[22] Tari Schreider, "Cybersecurity Law, Standards and Regulations, 2nd Edition," Rothstein Publishing; February 2020. [Online]. Available: https://www.ebooks.com/en-ua/book/209962921/cybersecurity-law-standards-and-regulations-2nd-edition/schreider-tari/?src=feed&gclid=CjwKCAjwyo36BRAXEiwA24CwGXnZH2wh9MpES6XqZ1aTj7qPkIBoX2douv55V34EXIxH8oRpwj3CpBoC1mAQAvD_BwE. Accessed on: 29.06.2020 (in English)
[23] PriceWaterhouseCooper (PwC). "Global Economic Crime and Fraud Survey 2018: Ukrainian findings Pulling fraud out of the shadows." [Online]. Available:
https://www.pwc.com/ua/en/survey/2018/pwc-gecs-2018-eng.pdf Accessed on: 13.04.2020 (in English)
[24]J. Clement, "IC3: total damage caused by reported cyber crime 2001-2019," In: Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2019 (in million U.S. dollars). [Online]. Available: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/#statisticContainer . Accessed on: 15.04.2020 (in English)
[25] Ukrainian-American University Bachelor Programs Catalog 2019-2020. [Online]. Available: https://www.concordia.edu.ua/wp-content/uploads/2020/02/2020-bba-catalog.pdf.
Accessed on: 02.03.2020 (in English)
[26] Ukrainian-American University Master's Degree Programs Catalog 2019-2020. [Online]. Available: https://www.concordia.edu.ua/wp-content/uploads/2019/07/ConcordiaUA-MBA-Catalog-Updated.pdf. Accessed on: 02.03.2020 (in English)
[27] M. Rouse, "What is Cybersecurity? Everything You Need to Know." [Online]. Available: https://searchsecurity.techtarget.com/definition/cybersecurity. Accessed on: 25.05.2020 (in English)
[28] Kevin Helms, "Jim Rogers Discusses Bitcoin as Money and Why Governments Will Stop Crypto." [Online]. Available:https://news.bitcoin.com/jim-rogers-bitcoin/. Accessed on: 21.07.2020 (in English)
[29] BuiltIn Journal, "Blockchain. What Is Blockchain Technology? How Does Blockchain Work?"
[Online]. Available: https://builtin.com/blockchain. Accessed on: 21.07.2020 (in English)
[30] CBInsights, "How Blockchain Technology Could Disrupt Real Estate." [Online]. Available: https://www.cbinsights.com/research/blockchain-real-estate-disruption/. Accessed on: 21.07.2020 (in English)
[31] Tia Vialva, "3D Hubs 3D Printing Trends Report Forecasts 24% Growth in 3D Printing Industry over 5 Years." [Online]. Available: https://3dprintingindustry.com/news/3d-hubs-3dprinting-trends-report-forecasts-24-growth-in-3d-printing-industry-over-5-years-167998/. Accessed on: 21.07.2020 (in English)
[32] Statista Research Department, May 11, 2020 "3D printing industry - worldwide market size 2020-2024." [Online]. Available https://www.statista.com/statistics/315386/global-market-for-3dprinters/. Accessed on: 21.07.2020 (in English)