КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.118.124137
УДК 001.89:004.056

Соколов Володимир Юрійович
кандидат технічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

ПІДХОДИ ДО ФОРМУВАННЯ НАУКОВОГО МИСЛЕННЯ У ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ З КІБЕРБЕЗПЕКИ

Анотація. Потреба в спеціалістах з розробки інформаційних систем зростає, тому збільшується вартість і попит на навчальні програми та курси «швидкого» входу в спеціальність. Підготовка спеціалістів з інформаційної безпеки неможлива без актуальних і чітких стандартів і програм навчання. На даний момент не існує чіткого стандарту для спеціальності «Кібербезпека» для докторів філософії. Публічний дискурс з приводу розробки та переробки паспортів спеціальностей має актуалізувати проблематику та виклики сучасного світового ринку інформаційних технологій. Застосування кращих практик у державних установах та службах дозволить укріпити безпеку української держави. В даній статті використовується досвід роботи зі здобувачами вищої освіти на різних рівнях. В якості об'єкту дослідження використовується корпус публікацій автора статті за останні шість років. Основними методами дослідження є критичний аналіз підходів до активізації творчих підходів у здобувачів; порівняльний аналіз складностей при підготовці до експерименту і класифікація публікацій за напрямками досліджень. В роботі представлений огляд ринку праці з інформаційної безпеки, його структура та особливості взаємодії роботодавців та претендентів на посаду. Окремо розглянуто особливості розвитку спеціалістів з інформаційної безпеки, а також їх фази формування. Консолідація університетських навчальних програм та порівняння паспортів наукових спеціальностей (05.13.21 — системи захисту інформації, 21.05.01 — інформаційна безпека, 05.13.06 — інформаційні технології, 13.00.10 — інформаційно-комунікаційні технології в освіті) докторів філософії дало можливість виокремити основні напрямки, які має знати та вміти випускник спеціальності «Кібербезпека». Окремим блоком розглянуті методики залучення до активного навчання студентів та аспірантів. Проаналізована статистика співпраці із здобувачами та показано, що покриття всіх аспектів кібербезпеки не завжди є можливим.

Ключові слова: кібербезпека; інформаційні технології; IT; захист інформації; паспорт спеціальності; CDIO; навчальний процес.

ВСТУП

Розвиток інформаційних технологій призводить до збільшення інформатизації суспільства. Потреба в спеціалістах з розробки інформаційних систем зростає, тому збільшується вартість і попит на навчальні програми та курси «швидкого» входу в спеціальність. Комплексність таких курсів не дає можливості використовувати розробника зразу після навчання в повну міру [1].

Постановка проблеми. Підготовка спеціалістів з інформаційної безпеки неможлива без актуальних і чітких стандартів і програм навчання. На даний момент не існує чіткого стандарту для спеціальності «Кібербезпека» для докторів філософії. Публічний дискурс з приводу розробки та переробки паспортів спеціальностей має

актуалізувати проблематику та виклики сучасного світового ринку інформаційних технологій. Застосування кращих практик у державних установах та службах дозволить укріпити безпеку української держави.

Аналіз останніх досліджень і публікацій. В роботі [2] розглянутий процес захисту інформаційної мережі закладу вищої освіти від зовнішніх загроз. Показані ризики, що виникають для студентів, викладачів та керівництва. Але не показано, як можна залучати студентів та аспірантів спеціальності «Кібербезпека» до покращення якості захисту інформаційних мереж та систем.

Проблематика захисту глобальних інформаційних мереж показана в [3]. Запропоновані елементи покращення навчання студентів з інформаційної безпеки, але не подано комплексної системи з формування стандартів. Хоча самі по собі загальні рекомендації можуть бути використані в майбутньому при розробці начальних програм для формування списку компетенцій.

Окремо слід зазначити практичний вклад роботи [4] на формування комплексного підходу при навчанні студентів розрахунку ризиків для інформаційних систем. Жодна серйозна фінансова установа не зможе довго зберігати стабільність роботи без виваженої методики оцінювання ризиків. Принципи розробки програм дисциплін «Теорія ризиків» та «Теорія прийняття рішень» можуть бути використані для формування програм інших учбових дисциплін згідно з стандартом спеціальності. В роботі [5] показаний частковий випадок SWOT-аналізу, як приклад практичного застосування цього інструментарію для формування практичних навичок у студентів.

Дослідження має на **меті** виявити кращі практики в для навчання здобувачів вищої освіти та сформувати підходи щодо стимулювання зацікавленості студентів та аспірантів в проведені практичних дослідів.

МЕТОДИКА ДОСЛІДЖЕННЯ

В даній статті використовується досвід роботи зі здобувачами вищої освіти на різних рівнях. В якості об’єкту дослідження використовується корпус публікацій автора статті за останні шість років. Основними методами дослідження є критичний аналіз підходів до активізації творчих підходів у здобувачів; порівняльний аналіз складностей при підготовці до експерименту і класифікація публікацій за напрямками досліджень.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Огляд запиту ринку праці з інформаційної безпеки

Існує кілька підходів до поступового залучання та розвитку людських ресурсів у продуктових компаніях. Це залежить від внутрішніх ресурсів компаній. Можна виділити п’ять категорій компаній:

1. Стартапи.
2. Невеликі з інтенсивною динамікою росту.
3. Середні зі сталим розвитком.
4. Великі аутсорсингові та аутстафінгові (так звані «галери»).
5. Міжнародні продуктові компанії.

Стартапи, або гаражні компанії, теж в свою чергу можуть існувати на різних рівнях та етапах залучення інвестицій. Але основною особливістю є їхня залежність від

професіоналів, які мають різноплановий досвід, гнучкість мислення та універсальність. Гарно розвинуті комунікаційні навички (soft skills) з одного боку дають якісний поштовх для розвитку, а, з іншого боку, мають великий ризик при втраті кожного члена команди навіть на короткотривалий термін. Такий тип спеціалістів не потребує комплексних навчальних програм, а лише окремих курсів для закриття пробілів в знаннях. Такі спеціалісти мають високий рівень автономності та рефлексії, тому можуть обирати стратегію свого розвитку самостійно (іноді із залучення ментора).

Невеликі компанії з кінцевим продуктом та регулярним доходом вже мають можливість працювати в більш спокійному режимі. Деякі функції з підтримки та розвитку флагманського продукту вже передається на менш кваліфікованих розробників. На перший план виносяться процеси, які, з одного боку, сповільнюють розвиток компанії, а, з іншого, дозволяють зменшити ризики, пов'язані із «текучкою» кадрів. Такі компанії вже можуть собі дозволити мінімальний розвиток персоналу з урахуванням персональних пробілів в знаннях та побажаннях окремих працівників. Але рушійною силою при виборі робітниками таких компаній є в першу чергу інтенсивне здобуття досвіду в технологіях та методах роботи. Такий підхід в балансі персонального розвитку та досвіду є оптимальними для початківців.

Середні компанії мають довгострокові контракти, тому зазвичай розвивають лінійку продуктів. При конвеєрному підході кількість продуктів, які потребують підтримку, збільшується. Компанія шукає різнопланових спеціалістів, які можуть мати нижчу кваліфікацію, але ціна помилки зменшується. Передача досвіду продовжується, але з меншою швидкістю, ніж в невеликих компаніях. Експертна база в таких компаніях більша, тому і можливостей для отримання досвіду теж більше, хоча передача знань розтягується на довший період часу. Такі компанії мають ресурси для проведення внутрішніх практикумів (workshops, townhalls, follow-ups), курсів із залученням внутрішніх або зовнішніх викладачів, підписок до навчальних онлайн платформ, додаткові бонуси на оплату підвищення кваліфікації.

Окремою когортою є компанії, основним ресурсом яких є кваліфіковані спеціалісти. Бізнес побудований на грамотному перепродажі людських ресурсів. Моделі найму аутсорс та аутстаф відрізняються не суттєво. Вони призводять до того, що компанія зацікавлена в окремих працівниках і готова вкладати ресурси в їх розвиток. Цей внесок має обмежену дію: зазвичай, обмежується технологічним стеком, який потрібний для конкретного проєкту або групи проєктів. Професійний ландшафт співробітників дуже різний. Він відрізняється за досвідом, спеціальностями, технологіями і навіть географією, тому дозволяю недорого організувати обмін досвідом в середині компанії. Основною особливістю є розділення на напрямки (домени) та окремі проєкти, що робить працівників відокремленими. Тому одна із найголовніших задач керівництва є зробити обмін досвідом легким та невимушеним. Лінійна комунікація (будь-хто може задати питання та очікувати, що йому дадуть відповідь), заохочення обміном досвідом (бонуси за проведення внутрішніх практикумів), обмін досвідом в середині спільнот (гільдій), ранжування на рівні (джун-міддл-сеньор), спонукання до підвищення рівня та достатні бюджети дозволяють збільшувати професійний потенціал компанії. Треба зауважити, що ці можливості в повній мірі відкриваються лише для проактивних співробітників.

Великі компанії та корпорації мають всі ресурси для розвитку персоналу, але використовують їх лише для мотивації співробітників, бо їм легше знайти на ринку праці нового спеціаліста з потрібними навичками та знаннями, ніж витрачати час на формування такого спеціаліста всередині компанії. Система побудована на повільному розвитку персоналу. Побудова кар'єри є розтягнутою у часі. Підтримка флагманських

продуктів займає значний час та не потребує кардинальний інновацій. Крім окремих дослідницьких (фундаментальних і прикладних) та експериментальних підрозділів, компанії не сильно зацікавлені інвестувати в людський потенціал. Виключення становлять деякі японські та німецькі компанії, але глобалізація розмиває їх локальний менталітет.

Особливості розвитку спеціалістів з інформаційної безпеки

Перераховані в попередньому розділі варіанти розвитку співробітників відносяться до всіх ІТ спеціальностей, тому розглядити спеціалістів з безпеки як окрему підгрупу спеціалістів не є коректним. Є особливості відокремлення окремих офіцерів з безпеки чи підрозділів забезпечення безпеки підприємств, але принципові можливості кар'єрного зросту не відрізняються. Різниця прослідковується в структурі отриманих знань.

Для звичайних ІТ спеціалістів навчальні курси привалюють на початку кар'єри, поступово збільшується кількість точкових практикумів та коротких програм по залученню до окремих технологій (фреймворків, методик, шаблонів, кращих практик тощо). Сертифікація з пройденими курсами бажана, але не є обов'язковою.

Для спеціалістів з інформаційної безпеки структура підвищення кваліфікації є здебільшого точковою, а сертифікація носить системних характер. Вартість та затребуваність сертифікованого спеціаліста значно вища.

Окремо стоїть питання базової освіти для всіх ІТ спеціалістів. Для формування комплексного уявлення про фізичні принципи та архітектуру технічних систем найкраще підходять перші загальнотехнічні курси в великих технічних закладах вищої освіти. Старші курси бакалаврської програми (першого рівня вищої освіти) вже дозволяють студенту визначитися зі спеціалізацією, яка йому більше до вподоби.

Підходи до отримання магістерського ступеня (другого рівня вищої освіти) у північноєвропейських та американських студентів відрізняється від українських. Після закінчення бакалаврського курсу спеціаліст часто вибирає роботу. А на магістерський курс студент йде лише тоді, коли розуміє, як саме буде використовувати свої знання або вищий рівень кваліфікації для подальшого кар'єрного зростання. Часто вибір магістерської програми припадає на споріднену спеціальність. (Немає сенсу розглядати випадки, коли людина вирішує кардинально змінити свою кваліфікацію).

В українських реаліях студенти старших курсів бакалаврської програми з інформаційних технологій та безпеки вже мають часткову або повну зайнятість, що дозволяє їм швидше зрозуміти, чи хочуть вони продовжувати навчання, повністю залучитися в роботу або змінити спеціальність (спеціалізацію). Звичайно кількість магістрантів менша за кількість бакалаврантів. Але прослідкується закономірність, що студенти з інформаційної безпеки частіше вирішують продовжити своє навчання на цій же спеціальності, а студенти інших спеціальностей з інформаційних технологій та автоматизації вирішують поглибити свої знання в галузі безпеки.

В такому підході є сенс, бо щоб захищати якусь систему, треба досконально знати принципи її роботи, вузькі місця, розповсюдженість та режими експлуатації. В результаті ми отримуємо спеціаліста, який не тільки може виявити вразливості системи, але й запропонувати ефективні методи з вдосконалення системи. Принцип універсальності затребуваний в новітніх гнучких технологіях розробки програмного забезпечення (Agile-підхід). З іншого боку, той самий гнучкий підхід можна використати в навчанні спеціалістів, як показано в [6].

ISSN 2663 - 4023

Фази формування спеціаліста з кібербезпеки

Процес зрощення спеціаліста з кібербезпеки складається з кількох послідовних фаз:

1. Формування загального уявлення про математичні методи та фізичні процеси в складних системах.
2. Вступ до спеціальності максимально загальними мазками (на даному етапі проходить первинна фільтрація випадкових студентів).
3. Вивчення існуючих систем і підходів із забезпечення інформаційної та інших видів безпеки.
4. Творче переосмислення підходів та вразливостей існуючих систем.
5. Формування персональних методів та рекомендацій із забезпечення безпеки.

Якщо поділити ці етапи на програми навчання, то з першого по третій вкладаються бакалаврський програмі. Четвертий етап допомагає сформуватися магістрам, які можуть створювати свій персональний інструментарій для вирішення проблем. А п’ята фаза відповідає програмі підготовки докторів філософії з кіберпезпеки.

Консолідація університетських навчальних програм

Окремо варто зазначити, що об’єднання спеціальностей з безпеки в закладах вищої освіти призвело до спрощення сприйняття спеціальності як цілісного поняття. Принцип консолідації був впроваджений в 2015 році і показаний на рис. 1 [7]. Абітурієнту стало легше пояснити ціль та предмет вивчення на спеціальності «Кібербезпека», а роботодавцю не треба заглиблюватися в нюанси різних спеціальностей.

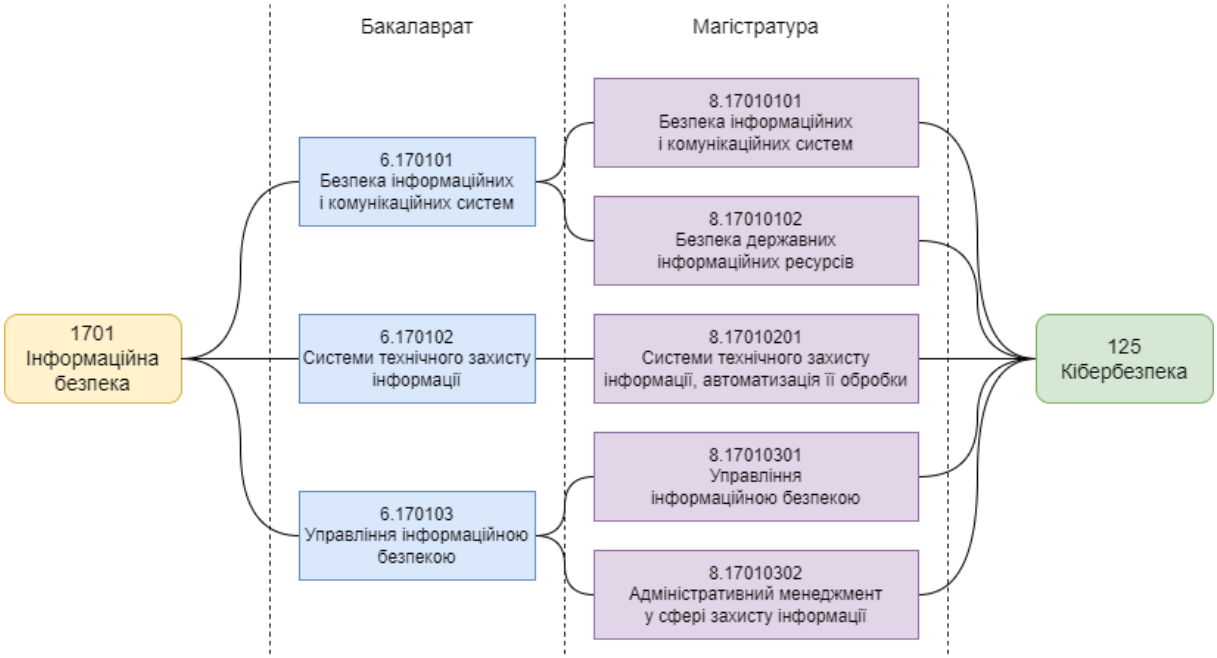

Рис. 1. Консолідація навчальних програм з інформаційної безпеки

З точки зору вищих навчальних закладів, які покривали кілька спеціальностей зі спектру безпеки, виникла можливість об’єднати колективи різних кафедр і відмовитися від дублювання схожих дисциплін на різних спеціальностях.

Для викладачів же принцип універсального викладення дисципліни спростив підготовку до занять і вивільнив час на додаткову паперову роботу з підготовки схожих за змістом навчальних програм.

Слід зауважити, що окрема спеціальність дозволила брати участь кільком українським університетам в міжнародних програмах з гармонізації магістерських програм для можливості в подальшому випускати спеціалістів з подвійними дипломами [8].

Порівняння паспортів наукових спеціальностей докторів філософії

Звичайно на даний момент ще не сформований загальний паспорт спеціальності «Кібербезпека» для докторів філософії, тому науковими радами використовуються попередньо розроблені паспорти спеціальностей для кандидатів та докторів наук.

Найкраще відповідають напрямку підготовки спеціальності:

- 05.13.21 — системи захисту інформації [9];
- 21.05.01 — інформаційна безпека держави [10].

Частково відповідають:

- 05.13.06 — інформаційні технології [11];
- 13.00.10 — інформаційно-комунікаційні технології в освіті [12].

Якщо порівняти предмет вивчення, то можна скласти матрицю відповідності, показану в табл. 1.

Таблиця 1

Порівняння спеціальностей на предмет їх вивчення

Код	**Предмет вивчення**	**Спеціальність**			
		05.13.21 — системи захисту інформації	21.05.01 — інформаційна безпека держави	05.13.06 — інформаційні технології	13.00.10 — інформаційно-комунікаційні технології в освіті
PR-1	Проблематика інформаційної безпеки	+	+	–	+
IS-1	Надійність інформаційних систем	+	–	+	–
IS-2	Стійкість інформаційних систем	+	+	+	–
IS-3	Ефективність захисту інформації	+	+	–	–
IS-4	Функціональна безпека	+	–	+	–
CP-1	Комплексність захисту інформації	+	+	–	–
CP-2	Моделювання атак	+	+	–	–
CP-3	Механізми попередження	–	+	–	–
UR-1	Захист кінцевих користувачів	+	+	–	+
UR-2	Інформаційний вплив	–	+	–	–
CR-1	Криптозахист	+	–	–	–
CR-2	Криптоаналіз	+	–	–	–

Слід зазначити, що в інших галузях знань теж зустрічаються питання безпеки, наприклад:

- в філософських науках: 21.03.01 — гуманітарна і політична безпека держави [13];
- в економічних науках: 21.04.01 — економічна безпека держави [14];
- в інших технічних науках: 21.06.01 — екологічна безпека [15];
- і в проєктах: 08.081.12 — інформаційне право; право інтелектуальної власності [16].

Методики залучення до активного навчання спеціалістів з кібербезпеки

Як ми побачили раніше, в залежності від рівня здобувача можуть бути різні підходи щодо розвитку та вдосконалення практичних навичок. Але як показує багаторічна практика роботи зі студентами та аспірантами, найкращих практичних результатів можна досягти, якщо залучати здобувачів освіти не залежно від їх рівня до наукової роботи.

Слід зауважити, що рівні залучення та свобода дій можуть кардинально відрізнятися в залежності від особливостей здобувача.

Бакалавранти часто не розуміють ще, що саме від них вимагається, тому отримати якийсь притаманний результат можна лише залучаючи студентів до виконання вже існуючих робіт або із залученням до частково пророблених ідей. Найкращі результати отримуються при залучені студентів до атомарних задач зі зрозумілими строками реалізації та критеріями прийомки результатів роботи.

Магістранти, звичайно, більш активні та зацікавлені в дослідженнях, але досить не досвідчені в принципах постановки експерименту та викладення результатів роботи. Співпраця з магістрантами складається з процесу постійного корегування напрямку руху. Але результати дозволяють стверджувати, що якщо студенти зацікавлений тематикою, то продуктивність може бути шаленою. Складність полягає в дуже малому часі на проведення експерименту: не більше двох місяців в кінці першого семестру навчання або на початку другого.

Аспірантам потрібно давати якнайширшу свободу в виборі тематики дослідження. Але підчас виконання роботи все одно потрібний контроль. Найкраще себе зарекомендував метод маленьких кроків з атомарними результатами і регулярних зустрічей із розглядом отриманих результатів та постановкою наступних задач. Регулярність може варіюватися від одного до трьох тижнів (в залежності від завантаження аспіранта та супервайзера).

Не залежно від рівня здобувача спостерігаються проблеми з оформленням кінцевих результатів дослідження. Складності бувають двох типів: (1) структуризація результатів під вимоги періодичного видання або конференції та (2) переходи між викладенням окремих частин дослідження.

Гарні результати показують здобувачі, які нотують всі свої кроки при реалізації дослідів. В таких випадках викладення матеріалу має менше пробілів, а також можна виділити складні місця та підводне каміння підчас підготовки устаткування та при проведені експериментів.

Від супервайзера очікується не тільки направлення та корегування дій здобувача, але і більш ретельний контроль. Наприклад, не слід повністю довіряти приведеному матеріалу. Його слід ретельно перевіряти в тому числі й на різні форми плагіату. Автоматичні системи перевірки на плагіат, які офіційно використовуються в українських

закладах вищої освіти не завжди дозволять виявити плагіат при перекладі з іноземних мов. Тому детальне вичитування матеріалів допоможе виявити непритаманні даному конкретному здобувачу тексти (за стилістикою, рівнем знань, термінологією, посиланнями тощо).

Статистика співпраці із здобувачами вищої освіти

Для ілюстрації в даній статті приводяться результати співпраці автора із бакалаврантами, магістрантами та аспірантами за останні кілька років. Автор в кінці 2019 року здобув науковий ступень кандидата технічних наук, тому перейшов з роботи з бакалаврантами та магістрами на роботу з магістрами та аспірантами. Тому в табл. 2 прослідковується зсув вправо.

Таблиця 2

Співавторство зі здобувачами освіти за останні шість років

Рік	Бакалаврanti	Магістранти	Аспіранти
2017	—	1	—
2018	2	2	—
2019	1	5	—
2020	—	4	—
2021	—	2	3
2022	—	1	7
Разом	3	15	10

Якщо попередні результати роботи були цікаві здобувачу, то при переході здобувача з одного рівня освіти на інший співпраця продовжується. Тематика роботи може змінюватися, але принципи співпраці лишаються тими самими.

Для простоти переходу від вивчення навчальної дисципліни до наукової роботи на кафедрі використовується підхід CDIO (Conceive-Design-Implement-Operate ‘вигадуй-розробляй-впроваджуй-керуй’) [17].

Роботи можна розділити за принципом послідовності або за тематикою розробки згідно кодуванню, наведеному в табл. 1:

1. *Безпека безпроводових технологій*, що відповідає критеріям IS-1 [18] – [20], IS-2 [21], IS-3 [22] – [24], CP-1 [25], [26] та CP-2 [27] – [30].
2. *Соціальний інжиніринг*, що відповідає критеріям UR-1 [31] та UR-2 [32] – [34].
3. *Обробка природної мови*, що відповідає критеріям CP-3 [35] – [39] та UR-2 [40].
4. *Безпека мозкової діяльності*, що відповідає критеріям UR-1 [41] і IS-4 [42].
5. *Інші*: криптопротоколи відповідають критерію CR-1 [43], профілювання користувачів — UR-1 [44] й аудит інфраструктури — CP-3 [45].

Через складність постановки експерименту не покритими лишаються лише напрямки проблематики інформаційної безпеки (PR-1) та криптоаналізу (CR-2).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В роботі представлений огляд ринку праці з інформаційної безпеки, його структура та особливості взаємодії роботодавців та претендентів на посаду. Окремо розглянуто особливості розвитку спеціалістів з інформаційної безпеки, а також їх фази формування.

Консолідація університетських навчальних програм та порівняння паспортів наукових спеціальностей докторів філософії дало можливість виокремити основні

напрямки, які має знати та вміти випускник спеціальності «Кібербезпека». Окремим блоком розглянуті методики залучення до активного навчання студентів та аспірантів. Проаналізована статистика співпраці із здобувачами та показано, що покриття всіх аспектів кібербезпеки не завжди є можливим. Тому найкращим є варіант багатопланової роботи викладачів, наукових співробітників, докторантів, аспірантів і студентів в рамках однієї наукової тематики. Таким чином, розподілення досвіду стає рівномірним, виникає конкурентне середовище, а кількість ідей та гіпотез збільшується.

План на подальше дослідження є порівняльний аналіз підходів активізації наукових досліджень серед студентів та аспірантів різних технічних спеціальностей напрямку підготовки 12 — інформаційні технології.

ПОДЯКА

Автор даної публікації висловлює подяку Володимиру Леонідовичу Бурячку, завідувачу кафедри інформаційної та кібернетичної безпеки (Державний університет телекомунікацій та Київський університет імені Бориса Грінченка), який був безпосереднім керівником і впроваджувачем інноваційних методів в навчанні, а також активно надихав і залучав студентів до наукової роботи [46], [47].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Buriachok, V., *et al.* (2020). Application of Ni Multisim Environment in the Practical Skills Building for Students of 125 “Cybersecurity” Specialty. *Cybersecurity: Education, Science, Technique*, *1*(*9*), 159–169. https://doi.org/10.28925/2663-4023.2020.9.159169

2 Nashynets-Naumova, A., *et al.* (2020). Technology for Information and Cyber Security in Higher Education Institutions of Ukraine. *Information Technologies and Learning Tools*, *77*(*3*), 337–354. https://doi.org/10.33407/itlt.v77i3.3424

3 Buriachok, V., *et al.* (2018). Training Model for Professionals in the Field of Information and Cyber Security in the Higher Educational Institutions of Ukraine. *Information Technologies and Learning Tools*, *67*(*5*), 277–291. https://doi.org/10.33407/itlt.v67i5.2347

4 Buriachok, V., *et al.* (2021). Interdisciplinary Approach to the Development of Is Risk Management Skills on the Basis of Decision-Making Theory. *Cybersecurity: Education, Science, Technique*, *3*(*11*), 155–165. https://doi.org/10.28925/2663-4023.2021.11.155165

5 Shevchenko, S., *et al.* (2020). Conducting a Swot-Analysis of Information Risk Assessment as a Means of Formation of Practical Skills of Students Specialty 125 Cyber Security. *Cybersecurity: Education, Science, Technique*, *2*(*10*), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168

6 Delhij, A., van Solingen, R., Wijnands, W. (2019). Керівництво по eduScrum : «Правила гри» (В. Соколов, Пер.). КУБГ.

7 Наказ «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року №266», №1460/27905 (2015). https://zakon.rada.gov.ua/rada/show/z1460-15

8 Yevdokymenko, M., Sokolov, V. (2019). Overview of the Course in “Wireless and Mobile Security.” *Educating the Next Generation MSc in Cyber Security*, 104–119. https://doi.org/10.5281/zenodo.2647747

9 Паспорт спеціальності «05.13.21 — системи захисту інформації», №26-08/2 (1999). https://zakon.rada.gov.ua/rada/show/v08_2330-99

10 Паспорт спеціальності «21.05.01 — інформаційна безпека держави», №9-10\8-т (2000).

11 Паспорт спеціальності «05.13.06 — інформаційні технології», №47-08/6 (2007). https://zakon.rada.gov.ua/rada/show/v0047330-07

12 Паспорт спеціальності «13.00.10 — інформаційно-комунікаційні технології в освіті», №200-06/1 (2009). https://zakon.rada.gov.ua/rada/show/v200-330-09

13 Паспорт спеціальності «21.03.01 — гуманітарна і політична безпека держави (філософські науки)», №11-10/11т (2004). https://zakon.rada.gov.ua/rada/show/v0_11330-04
14 Паспорт спеціальності «21.04.01 — економічна безпека держави (економічні науки)», №11-10/11т (2004). https://zakon.rada.gov.ua/rada/show/va11-330-04
15 Паспорт спеціальності «21.06.01 — екологічна безпека», №33-07/7 (2001). https://zakon.rada.gov.ua/rada/show/va7_7330-01
16 Пилипчук, В., Доронін, І. (2018). Право національної безпеки та військове право: теоретичні та прикладні засади становлення і розвитку в Україні. *Інформація і право*, *2*(*25*), 62–72. http://ippi.org.ua/sites/default/files/8_8.pdf
17 CDIO office (2019). Ініціатива CDIO (В. Соколов, Пер.). КУБГ. http://www.cdio.org/files/CDIO_standards_ua.pdf
18 Bogachuk, I., Sokolov, V., Buriachok, V. (2018). Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers. In *V International Scientific and Practical Conference Problems of Infocommunications. Science and Technology* (pp. 581–585). https://doi.org/10.1109/infocommst.2018.8632151
19 Hu, Z., *et al.* (2020). Bandwidth Research of Wireless IoT Switches. In *15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering* (pp. 546–550). https://doi.org/10.1109/tcset49122.2020.235492
20 Hu, Z., *et al.* (2020). Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range. *Data-Centric Business and Applications*, *48*, 675–709. https://doi.org/10.1007/978-3-030-43070-2_29
21 Владимиренко, М., Соколов, В., Астапеня, В. (2019). Дослідження стійкості роботи однорангових безпроводових мереж із самоорганізацією. *Кібербезпека: освіта, наука, техніка*, *3*, 6–26. https://doi.org/10.28925/2663-4023.2019.3.626
22 Kipchuk, F., *et al.* (2020). Investigation of Availability of Wireless Access Points based on Embedded Systems. In *VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology* (pp. 246–250). https://doi.org/10.1109/picst47496.2019.9061551
23 Соколов, В., Вовкотруб, Б., Зоткін, Є. (2019). Порівняльний аналіз пропускної здатності малопотужних безпроводових IoT-комутаторів. *Кібербезпека: освіта, наука, техніка*, *1*(*5*), 16–30. https://doi.org/10.28925/2663-4023.2019.5.1630
24 Биць, А., *et al.* (2021). Експериментальне визначення оптимальних параметрів роботи телеконференції на мобільних пристроях. *Кібербезпека: освіта, наука, техніка*, *2*(*14*), 68–86. https://doi.org/10.28925/2663-4023.2021.14.6886
25 Taj Dini, M., Sokolov, V. (2017). Internet of Things Security Problems. *Сучасний захист інформації*, *1*, 120–127.
26 Vladymyrenko, M., *et al.* (2019). Analysis of Implementation Results of the Distributed Access Control System. In *VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology* (pp. 39–44). https://doi.org/10.1109/picst47496.2019.9061376
27 Taj Dini, M., Sokolov, V. (2018). Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio. *Сучасний захист інформації*, *1*, 82–89.
28 TajDini, M., Sokolov, V., Buriachok, V. (2019). Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio. In *8th International Conference on "Mathematics. Information Technologies. Education"* (pp. 287–296).
29 Buriachok, V., Sokolov, V., Taj Dini, M. (2020). Research of Caller ID Spoofing Launch, Detection, and Defense. *Cybersecurity: Education, Science, Technique*, *1*(*7*), 6–16. https://doi.org/10.28925/2663-4023.2020.7.616
30 TajDini, M., Sokolov, V., Skladannyi, P. (2021). Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio. In *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics* (pp. 7–11). https://doi.org/10.1109/ukrmico52950.2021.9716665
31 Sokolov, V., Korzhenko, O. (2018). Analysis of Recent Attacks based on Social Engineering Techniques. In *Всеукраїнська науково-практична конференція здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації»* (pp. 361–363). https://doi.org/10.2139/ssrn.3455471
32 Соколов, В., Курбанмурадов Д. (2018). Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. *Кібербезпека: освіта, наука, техніка*, *1*, 6–16. https://doi.org/10.28925/2663-4023.2018.1.616

33 Marusenko, R., Sokolov, V., Buriachok, V. (2020). Experimental Evaluation of Phishing Attack on High School Students. *Advances in Computer Science for Engineering and Education III*, *1247*, 668–680. https://doi.org/10.1007/978-3-030-55506-1_59
34 Marusenko, R., Sokolov, V., Bogachuk, I. (2022). Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation. *Advances in Artificial Systems for Logistics Engineering*, *135*, 583–594. https://doi.org/10.1007/978-3-031-04809-8_53
35 Iosifova, O., *et al.* (2020). Techniques Comparison for Natural Language Processing. In *2nd International Workshop on Modern Machine Learning Technologies and Data Science* (pp. 57–67).
36 Iosifov, I., Iosifova, O., Sokolov, V. (2020). Sentence Segmentation from Unformatted Text using Language Modeling and Sequence Labeling Approaches. In *VII International Scientific and Practical Conference Problems of Infocommunications. Science and Technology* (pp. 335–337). https://doi.org/10.1109/picst51311.2020.9468084
37 Romanovskyi, O., *et al.* (2020). Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition. *Advances in Computer Science for Engineering and Education IV*, *83*, 25–36. https://doi.org/10.1007/978-3-030-80472-5_3
38 Iosifova, O., *et al.* (2021). Analysis of Automatic Speech Recognition Methods. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems* (pp. 252–257).
39 Iosifov, I., *et al.* (2022). Natural Language Technology to Ensure the Safety of Speech Information. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II* (pp. 216–226).
40 Iosifov, I., *et al.* (2022). Transferability Evaluation of Speech Emotion Recognition Between Different Languages. *Advances in Computer Science for Engineering and Education*, *134*, 413–426. https://doi.org/10.1007/978-3-031-04812-8_35
41 TajDini, M., *et al.* (2020). Wireless Sensors for Brain Activity — A Survey, *Electronics*, *9*(*12*), 1–26. https://doi.org/10.3390/electronics9122092
42 Hu, Z., *et al.* (2021). Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence. *Advances in Computer Science for Engineering and Education IV*, *83*, 374–388. https://doi.org/10.1007/978-3-030-80472-5_31
43 Курбанмурадов, Д., Соколов, В., Астапеня, В. (2019). Реалізація протоколу шифрування XTEA на базі безпроводових систем стандарту IEEE 802.15.4. *Кібербезпека: освіта, наука, техніка*, *2*(*6*). 32–45. https://doi.org/10.28925/2663-4023.2019.6.3245
44 Цирканюк, Д., *et al.* (2021). Метод побудови профілів користувача маркетплейсу і зловмисника. *Кібербезпека: освіта, наука, техніка*, *2*(*14*), 50–67. https://doi.org/10.28925/2663-4023.2021.14.5067
45 Kipchuk, F., *et al.* (2021). Assessing Approaches of IT Infrastructure Audit. In *8th International Conference on Problems of Infocommunications, Science and Technology* (pp. 213–217). https://doi.org/10.1109/picst54195.2021.9772181
46 Buriachok, V., Sokolov, V. (2019). Implementation of Active Learning in the Master's Program on Cybersecurity. *Advances in Computer Science for Engineering and Education II*, *938*, 610–624. https://doi.org/10.1007/978-3-030-16621-2_57
47 Buriachok, V., Shevchenko, S., Skladannyi, P. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of Students. *Cybersecurity: Education, Science, Technique*, *2*(*2*), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023

Volodymyr Y. Sokolov
Ph.D., associate professor,
associate professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

APPROACHES TO THE FORMATION OF SCIENTIFIC THINKING IN CYBERSECURITY HIGH SCHOOL STUDENTS

Abstract. The need for specialists in the development of information systems is growing, therefore the cost and demand for educational programs and courses for "quick" entry into the specialty is increasing. Training of information security specialists is impossible without current and clear standards and training programs. Currently, there is no clear standard for a Cybersecurity major for Ph.D. The public discourse on the development and processing of passports of specialties should actualize the problems and challenges of the modern world market of information technologies. The application of best practices in state institutions and services will strengthen the security of the Ukrainian state. This article uses the experience of working with students of higher education at different levels. The corpus of the author's publications over the past six years is used as the object of the research. The main research methods are a critical analysis of approaches to the activation of creative approaches in acquirers; comparative analysis of difficulties in preparing for the experiment and classification of publications by research areas. The work presents an overview of the information security labor market, its structure and features of interaction between employers and job applicants. The peculiarities of the development of information security specialists, as well as their phases of formation, are considered separately. Consolidation of university curricula and comparison of passports of scientific specialties (05.13.21 information protection systems, 21.05.01 information security, 05.13.06 information technologies, 13.00.10 information and communication technologies in education) of doctors of philosophy made it possible to single out the main directions, which a graduate of the "Cybersecurity" specialty should know and be able to do. Methods of involving students and graduate students in active learning are considered in a separate block. Statistics of cooperation with acquirers are analyzed, and it is shown that covering all aspects of cybersecurity is not always possible.

Keywords: cyber security; information technology; IT; information protection; specialty passport; CDIO; learning process.

REFERENCES

1 Buriachok, V., *et al.* (2020). Application of Ni Multisim Environment in the Practical Skills Building for Students of 125 "Cybersecurity" Specialty. *Cybersecurity: Education, Science, Technique, 1*(*9*), 159–169. https://doi.org/10.28925/2663-4023.2020.9.159169

2 Nashynets-Naumova, A., *et al.* (2020). Technology for Information and Cyber Security in Higher Education Institutions of Ukraine. *Information Technologies and Learning Tools*, *77*(*3*), 337–354. https://doi.org/10.33407/itlt.v77i3.3424

3 Buriachok, V., *et al.* (2018). Training Model for Professionals in the Field of Information and Cyber Security in the Higher Educational Institutions of Ukraine. *Information Technologies and Learning Tools*, *67*(*5*), 277–291. https://doi.org/10.33407/itlt.v67i5.2347

4 Buriachok, V., *et al.* (2021). Interdisciplinary Approach to the Development of Is Risk Management Skills on the Basis of Decision-Making Theory. *Cybersecurity: Education, Science, Technique*, *3*(*11*), 155–165. https://doi.org/10.28925/2663-4023.2021.11.155165

5 Shevchenko, S., *et al.* (2020). Conducting a Swot-Analysis of Information Risk Assessment as a Means of Formation of Practical Skills of Students Specialty 125 Cyber Security. *Cybersecurity: Education, Science, Technique*, *2*(*10*), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168

6 Delhij, A., van Solingen, R., Wijnands, W. (2015). The eduScrum Guide "The rules of the Game."

7 Order "On the Specifics of the Introduction of the List of Fields of Knowledge and Specialties for which Higher Education Applicants are Trained, Approved by the Resolution of the Cabinet of Ministers of

Ukraine dated April 29, 2015 No. 266," #1460/27905 (2015). https://zakon.rada.gov.ua/rada/show/z1460-15

8 Yevdokymenko, M., Sokolov, V. (2019). Overview of the Course in "Wireless and Mobile Security." *Educating the Next Generation MSc in Cyber Security*, 104–119. https://doi.org/10.5281/zenodo.2647747

9 Specialty passport "05.13.21 Information Protection Systems," #26-08/2 (1999). https://zakon.rada.gov.ua/rada/show/v08_2330-99

10 Specialty passport "21.05.01 Information Security of the State," #9-10\8-t (2000).

11 Specialty passport "05.13.06 Information Technologies," #47-08/6 (2007). https://zakon.rada.gov.ua/rada/show/v0047330-07

12 Specialty passport "13.00.10 Information and Communication Technologies in Education," #200-06/1 (2009). https://zakon.rada.gov.ua/rada/show/v200-330-09

13 Specialty passport "21.03.01 Humanitarian and Political Security of the State (Philosophical Sciences)," #11-10/11t (2004). https://zakon.rada.gov.ua/rada/show/v0_11330-04

14 Specialty passport "21.04.01 Economic Security of the State (Economic Sciences)," #11-10/11t (2004). https://zakon.rada.gov.ua/rada/show/va11-330-04

15 Specialty passport "21.06.01 Environmental Safety," #33-07/7 (2001). https://zakon.rada.gov.ua/rada/show/va7_7330-01

16 Pylypchuk, V., Doronin, I. (2018). National Security Law and Military Law: Theoretical and Applied Principles of Formation and Development in Ukraine. *Information and law*, *2*(*25*), 62–72. http://ippi.org.ua/sites/default/files/8_8.pdf

17 CDIO Office (2019). CDIO Standards 2.1. http://www.cdio.org/content/cdio-standards-21

18 Bogachuk, I., Sokolov, V., Buriachok, V. (2018). Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers. In *V International Scientific and Practical Conference Problems of Infocommunications. Science and Technology* (pp. 581–585). https://doi.org/10.1109/infocommst.2018.8632151

19 Hu, Z., *et al.* (2020). Bandwidth Research of Wireless IoT Switches. In *15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering* (pp. 546–550). https://doi.org/10.1109/tcset49122.2020.235492

20 Hu, Z., *et al.* (2020). Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range. *Data-Centric Business and Applications*, *48*, 675–709. https://doi.org/10.1007/978-3-030-43070-2_29

21 Vladymyrenko, M., Sokolov, V., Astapenia, V. (2019). Study of Stability of Peer-to-Peer Wireless Networks with Self-Organization. *Cybersecurity: Education, Science, Technique*, *3*, 6–26. https://doi.org/10.28925/2663-4023.2019.3.626

22 Kipchuk, F., *et al.* (2020). Investigation of Availability of Wireless Access Points based on Embedded Systems. In *VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology* (pp. 246–250). https://doi.org/10.1109/picst47496.2019.9061551

23 Sokolov, V., Vovkotrub, B., Zotkin, I. (2019). Comparative Analysis of Bandwidth of Low-Power Wireless IoT Switches. *Cybersecurity: Education, Science, Technique*, *1*(*5*), 16–30. https://doi.org/10.28925/2663-4023.2019.5.1630

24 Byts, A., *et al.* (2021). Experimental Determination of the Optimal Parameters of Teleconferencing on Mobile Devices. *Cybersecurity: Education, Science, Technique*, *2*(*14*), 68–86. https://doi.org/10.28925/2663-4023.2021.14.6886

25 Taj Dini, M., Sokolov, V. (2017). Internet of Things Security Problems. *Modern Information Protection*, *1*, 120–127.

26 Vladymyrenko, M., *et al.* (2019). Analysis of Implementation Results of the Distributed Access Control System. In *VI International Scientific and Practical Conference Problems of Infocommunications. Science and Technology* (pp. 39–44). https://doi.org/10.1109/picst47496.2019.9061376

27 Taj Dini, M., Sokolov, V. (2018). Penetration Tests for Bluetooth Low Energy and Zigbee using the Software-Defined Radio. *Modern Information Protection*, *1*, 82–89.

28 TajDini, M., Sokolov, V., Buriachok, V. (2019). Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio. In *8th International Conference on "Mathematics. Information Technologies. Education"* (pp. 287–296).

29 Buriachok, V., Sokolov, V., Taj Dini, M. (2020). Research of Caller ID Spoofing Launch, Detection, and Defense. *Cybersecurity: Education, Science, Technique*, *1*(*7*), 6–16. https://doi.org/10.28925/2663-4023.2020.7.616

30 TajDini, M., Sokolov, V., Skladannyi, P. (2021). Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio. In *IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics* (pp. 7–11). https://doi.org/10.1109/ukrmico52950.2021.9716665

31 Sokolov, V., Korzhenko, O. (2018). Analysis of Recent Attacks based on Social Engineering Techniques. In *All-Ukrainian scientific and practical conference of higher education graduates and young scientists "Computer engineering and cyber security: achievements and innovations"* (pp. 361–363). https://doi.org/10.2139/ssrn.3455471

32 Sokolov, V., Kurbanmuradov D. (2018). The Method of Combating Social Engineering at the Objects of Information Activity. *Cybersecurity: Education, Science, Technique, 1*, 6–16. https://doi.org/10.28925/2663-4023.2018.1.616

33 Marusenko, R., Sokolov, V., Buriachok, V. (2020). Experimental Evaluation of Phishing Attack on High School Students. *Advances in Computer Science for Engineering and Education III*, *1247*, 668–680. https://doi.org/10.1007/978-3-030-55506-1_59

34 Marusenko, R., Sokolov, V., Bogachuk, I. (2022). Method of Obtaining Data from Open Scientific Sources and Social Engineering Attack Simulation. *Advances in Artificial Systems for Logistics Engineering*, *135*, 583–594. https://doi.org/10.1007/978-3-031-04809-8_53

35 Iosifova, O., *et al.* (2020). Techniques Comparison for Natural Language Processing. In *2nd International Workshop on Modern Machine Learning Technologies and Data Science* (pp. 57–67).

36 Iosifov, I., Iosifova, O., Sokolov, V. (2020). Sentence Segmentation from Unformatted Text using Language Modeling and Sequence Labeling Approaches. In *VII International Scientific and Practical Conference Problems of Infocommunications. Science and Technology* (pp. 335–337). https://doi.org/10.1109/picst51311.2020.9468084

37 Romanovskyi, O., *et al.* (2020). Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition. *Advances in Computer Science for Engineering and Education IV*, *83*, 25–36. https://doi.org/10.1007/978-3-030-80472-5_3

38 Iosifova, O., *et al.* (2021). Analysis of Automatic Speech Recognition Methods. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems* (pp. 252–257).

39 Iosifov, I., *et al.* (2022). Natural Language Technology to Ensure the Safety of Speech Information. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II* (pp. 216–226).

40 Iosifov, I., *et al.* (2022). Transferability Evaluation of Speech Emotion Recognition Between Different Languages. *Advances in Computer Science for Engineering and Education*, *134*, 413–426. https://doi.org/10.1007/978-3-031-04812-8_35

41 TajDini, M., *et al.* (2020). Wireless Sensors for Brain Activity — A Survey, *Electronics*, *9*(*12*), 1–26. https://doi.org/10.3390/electronics9122092

42 Hu, Z., *et al.* (2021). Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence. *Advances in Computer Science for Engineering and Education IV*, *83*, 374–388. https://doi.org/10.1007/978-3-030-80472-5_31

43 Kurbanmuradov, D., Sokolov, V., Astapenia, V. (2019). Implementation of the XTEA Encryption Protocol based on Wireless Systems of the IEEE 802.15.4 Standard. *Cybersecurity: Education, Science, Technique*, *2*(*6*). 32–45. https://doi.org/10.28925/2663-4023.2019.6.3245

44 Tsyrkaniuk, D., *et al.* (2021). The Method of Building Profiles of the Marketplace User and the Attacker. *Cybersecurity: Education, Science, Technique*, *2*(*14*), 50–67. https://doi.org/10.28925/2663-4023.2021.14.5067

45 Kipchuk, F., *et al.* (2021). Assessing Approaches of IT Infrastructure Audit. In *8th International Conference on Problems of Infocommunications, Science and Technology* (pp. 213–217). https://doi.org/10.1109/picst54195.2021.9772181

46 Buriachok, V., Sokolov, V. (2019). Implementation of Active Learning in the Master's Program on Cybersecurity. *Advances in Computer Science for Engineering and Education II*, *938*, 610–624. https://doi.org/10.1007/978-3-030-16621-2_57

47 Buriachok, V., Shevchenko, S., Skladannyi, P. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of Students. *Cybersecurity: Education, Science, Technique*, *2*(*2*), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104