УДК 378.14

ПЕДАГОГІЧНИЙ ЗМІСТ ПІДГОТОВКИ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ

кандидат педагогічних наук, доцент, Самойленко О. О.

https://orcid.org/0000-0002-6374-4168

samoylenko_aleksey@outlook.com

Навчально-науковий інститут інформаційної безпеки Служби Безпеки України, Київ, Україна

У статті представлений аналітичний огляд педагогічного змісту підготовки бакалаврів з кібербезпеки. Досліджувались питання проблем безпеки комп'ютерних мереж українськими та зарубіжними вченими. Проаналізовано навчальні програми підготовки бакалаврів з кібербезпеки у Нью-Йорку, Франції, Україні та інших державах. Охарактеризовано підготовку фахівця за освітнім ступенем бакалавр з кібербезпеки є правом сучасної професійної діяльності у системі державних та комерційних підприємств, які пов'язані послугами щодо захисту інформації на об'єктах інформаційної діяльності. З'ясовано, що теоретичний зміст предметної області підготовки бакалаврів з кібербезпеки передбачає знання законодавчої, нормативно-правової бази та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності. Охарактеризовано компоненти освітньої програми та програмні результати підготовки бакалавра з кібербезпеки.

Ключові слова: професійна підготовка, бакалаври з кібербезпеки, зміст підготовки бакалавра з кібербезпеки.

Кандидат педагогических наук, доцент, Самойленко А. А., Педагогическое содержание подготовки бакалавров по

кибербезопасности / Учебно-научный институт информационной безопасности Службы безопасности Украины, Киев, Украина.

В статье представлен аналитический обзор педагогического содержания подготовки бакалавров по кибербезопасности. Исследовались вопросы проблем безопасности компьютерных сетей украинскими и зарубежными учеными. Проанализированы учебные программы подготовки бакалавров по кибербезопасности в Нью-Йорке, Франции, Украине и других государствах. Охарактеризованы подготовку специалиста по образовательным степенью бакалавр кибербезопасности является правом современной профессиональной деятельности в системе государственных и коммерческих предприятий, которые связаны услугами по защите информации на объектах информационной деятельности. Выяснено, что теоретическое содержание предметной области подготовки бакалавров по кибербезопасности предполагает знание законодательной, нормативно-правовой базы и требований соответствующих международных стандартов и практик по осуществлению профессиональной деятельности. Охарактеризованы компоненты образовательной программы и программные результаты подготовки бакалавра по кибербезопасности.

Ключевые слова: профессиональная подготовка, бакалавры по кибербезопасности, содержание подготовки бакалавра по кибербезопасности.

A. Samoylenko, PhD, Associate Professor, Pedagogical content of training bachelors in cybersecurity / Ukraine Educational and scientific institute of information security service, Kiev, Ukraine

The article presents an analytical review of the pedagogical content of cybersecurity training. Research into computer network security issues

Ukrainian and foreign scientists. The training programs for cybersecurity bachelors in New York, France, Ukraine and other countries are analyzed. The training of a Bachelor of Arts degree in cybersecurity is a right of modern professional activity in the system of state and commercial enterprises, which are connected with services in protection of information on objects of information activity. It is found that the theoretical content of the subject area of preparation of bachelors in cybersecurity requires knowledge of the legal, regulatory framework and requirements of the relevant international standards and practices for professional activity. The components of the educational program and program results of preparation of the bachelor's degree in cybersecurity are characterized.

Keywords: professional training, cybersecurity bachelors, content of cyber security bachelors training.

Вступ. Для захисту комп'ютерних мереж фахівцями з кібербезпеки незалежно від інформації, яка циркулює в них, слід спочатку зрозуміти, які інформаційні технології вони використовують та на яких принципах працюють. Забезпечення безпеки комп'ютерних мереж фахівцями з кібербезпеки вимагає, зокрема, знання з персонального захисту інформації, яке використовується підприємствами або окремими користувачами, поточних налаштувань відповідного такого захисту. Важливою проблемою безпеки комп'ютерних мереж є забезпечення прозорості дій, яка може вплинути на безпеку і надійність критично важливих інформаційних активів. Складність усунення цієї проблеми полягає в тому, що в мережах використовуються кілька різних комунікаційних протоколів [1]. Проблемою безпеки комп'ютерних мереж є неможливість забезпечення управління змінами та дотримання політики безпеки. Без системи запобігання неавторизованому доступу чи інформування

про нього, можна вільно отримати доступ до активу і змінити його налаштування.

Мета: аналітичний огляд педагогічного змісту підготовки бакалаврів з кібербезпеки, дослідження проблем безпеки комп'ютерних мереж українськими та зарубіжними вченими та аналіз навчальних програм підготовки бакалаврів з кібербезпеки.

Виклад основного матеріалу. Кібербезпека передбачає вирішення багатьох проблем, в тому числі й боротьба з комп'ютерними вірусами. Термін «комп'ютерний вірус» уперше вжив Ф. Коен у 1984 р. Він поділив віруси на такі групи:

1) ті, що написані для наукових досліджень у галузі інформатики;

2) так звані «дикі» віруси для заподіяння шкоди користувачам [2].

Написання вірусів набуває ознак промислового виробництва, їх кількість вимірюється десятками тисяч, і перед людством виникає проблема усвідомлення небезпечності цієї загрози. Кібербезпека стикнулася з тим, що групи кіберзлочинців стають все більш «корпоративними», та закладають в основу наступні аспекти:

- нові технології все частіше моделюють корпоративну ієрархію (у багатьох організаціях застосовуються так звані «шлюзи», що маскують шкідливу активність;
- це надає можливість кіберзлочинцям захоплювати кіберпростір та уникати виявлення);
- можливості та ризики хмарних технологій (багато хмарних застосунків, ініціаторами застосування яких є співробітники компанії з метою підвищення ефективності та пошуку нових бізнес-перспектив, зараховано до категорії підвищеного ризику);

– звичне рекламне прикладне забезпечення, що стає джерелом зараження більше половини мереж підприємств.

Забезпечення кібербезпеки є актуальним для багатьох сфер діяльності, зокрема, сфер науки, техніки та технологій (особливо інформаційних технологій), що охоплюють проблеми, пов'язані із захищеністю кіберпростору країни, окремих об’єктів його інфраструктури тощо [2]. Такими об'єктами, зокрема, є:

- інформаційно-технологічна підтримка кіберпростору країни (підприємства, установи тощо);

- інформаційні ресурси країни (підприємства, установи тощо);

- інформаційні та інтелектуальні системи різних класів;

- технології забезпечення кібербезпеки об'єктів різного рівня (система, об'єкт системи, компонент об'єкту тощо),

- процеси управління кібербезпекою об'єктів різної природи.

Згідно з даними, поданими Французьким агентством з питань мережевої та інформаційної безпеки та стратегією кібербезпеки у Канаді [3, 4], більше третини організацій, які піддалися кібератакам у 2016 р., повідомили про істотні втрати доходів, втрачені можливості та відтік замовників. Тому більшість цих організацій після таких атак стали вдосконалювати технології, методи, механізми та процедури захисту.

Зарубіжні фахівці з кібербезпеки, серед основних перешкод інформаційного захисту визначають: брак ресурсів; несумісність інформаційних систем та технологій захисту і недостатню кількість відповідних фахівців [5, 6]

Підготовка фахівця за освітнім ступенем бакалавр з кібербезпеки є правом сучасної професійної діяльності у системі державних та комерційних підприємств, які пов’язані послугами щодо захисту інформації на об’єктах інформаційної діяльності. Актуальність

проблем кібербезпеки підкреслюється необхідністю користування інформаційними системами та технологіями, від соціальних мереж, розміщення інформації про свої персональні дані в Інтернеті до користування банківськими рахунками, системами e-commerce та ін.

У навчальних програмах для підготовки бакалаврів з кібербезпеки у Нью-Йорку (асоціація обчислювальної техніки), зазначається, що інженери такого напрямку підготовки мають професійну підготовку в області електротехніки, програмного забезпечення та інтеграції апаратно-програмного забезпечення. Фахівці з кібербезпеки займаються різними аспектами обчислень: від проектування окремих мікропроцесорів, комп'ютерів і суперкомп'ютерів до захисту інформації на різних рівнях у кіберпросторі. Зазвичай завдання інженера з кібербезпеки може включати в себе написання програмного і мікропрограмного забезпечення для вбудованих мікроконтролерів, проектування надвеликих інтегральних схем, аналогових датчиків, плат змішаних сигналів, а також розробку операційних систем. Фахівці в області кібербезпеки також працюють над дослідженнями для робототехніки, які спираються на використанні цифрових систем для управління і контролю електричних систем, таких як двигуни, системи зв'язку, а також датчики [7].

Об’єкти професійної діяльності випускників спеціальності «кібербезпека»: об'єкти інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й інформаційні технології; технології забезпечення безпеки інформації об’єктів різного рівня (система, об’єкт системи, компонент об’єкта), що пов’язані з інформаційними, інформаційно-комунікаційними технологіями, що використовуються для

забезпечення функціонування цих об’єктів; процеси управління інформаційною і кібербезпекою об’єктів, що підлягають захисту.

Підготовка такого фахівця передбачає формування та розвиток професійних компетентностей щодо захисту інформації на об’єктах інформаційної діяльності; вивчення теоретичних та методичних положень, організаційних та практичних інструментів зі спеціальності кібербезпеки; методики та технології забезпечення безпеки інформації.

Теоретичний зміст предметної області підготовки бакалаврів з кібербезпеки передбачає знання законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності. Також сюди можна віднести принципи супроводу систем та комплексів інформаційної та/або кібербезпеки, теорії, моделей та принципів управління доступом до інформаційних ресурсів та теорії систем управління інформаційною та/або кібербезпекою [1].

Робота фахівця з кібербезпеки із засобами виявлення, управління та ідентифікації ризиків підводить до високого рівня оцінювання та забезпечення необхідного ступеня захищеності інформації. Використання сучасних інформаційно-комунікаційних технологій вимагає від таких фахівців відповідних знань методів та засобів технічного та криптографічного захисту інформації, сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій та автоматизованих систем проектування.

Освітня програма передбачає обов’язкове професійне навчання з метою отримання бакалавром кваліфікації фахівця захисту інформації в інформаційних і комунікаційних системах. Передбачена практика, з метою забезпечення умов підготовки фахівця в реальному середовищі майбутньої професійної діяльності. Залучення до

викладацької діяльності керівників та професіоналів, які працюють в системі професійної освіти та на виробництві в галузі захисту інформації, а також представників бізнесу, з метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу. Реалізація процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін. Рекомендується реалізація студентської мобільності, академічної співпраці та молодіжних обмінів.

Випускник є придатним для працевлаштування на підприємствах, в організаціях та установах на яких обробляєтеся інформація з обмеженим доступом, що займаються розробкою та супроводом програмного забезпечення захисту інформації. Компоненти освітньої програми логічно поділяються на обов'язкові та вибіркові (Рис. 2.).

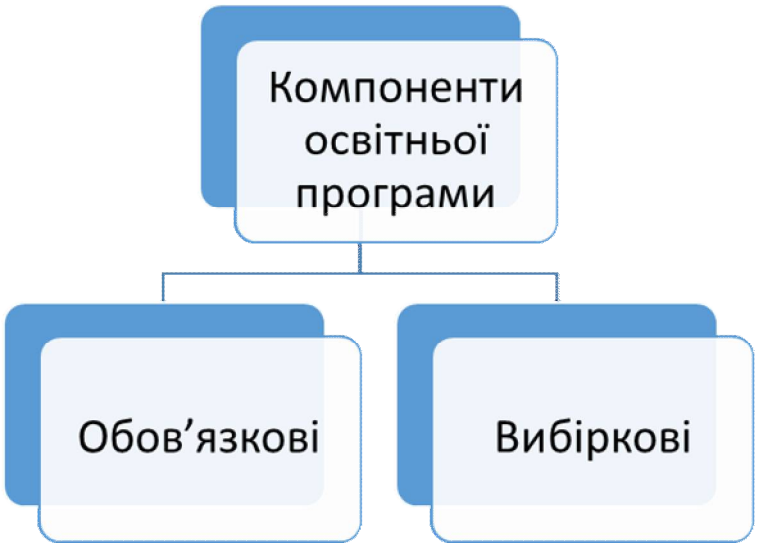

Рис. 2.1. Компоненти освітньої програми

Розглянемо компоненти освітньо-професійної програми та їх логічну послідовність.

Такий компонент, як історія України, української культури має п'ять кредитів. Українська мова (за професійним спрямуванням),

філософія та іноземна мова містять по три кредити. Вища математика складає 20 кредитів, фізика – 11, Інформаційні технології – 5. Теорія ймовірностей та математична статистика і дискретна математика містять по три кредити. Технології програмування уміщують 12 кредитів. Основи теорія кіл, сигналів та процесів в електроніці, операційні системи та електроніка складаються з чотирьох кредитів кожна. Архітектура комп'ютерних систем має три кредити. Інформаційно-комунікаційні системи – 9, теорія інформації та кодування – 6 прикладна криптологія – 9, нормативно-правове забезпечення інформаційної безпеки – 3, системи технічного захисту інформації – 4, захист інформації в інформаційно-комунікаційних системах – 11, комплексні системи захисту інформації: проектування, впровадження, супровід – 10, управління інформаційною безпекою – 3, екологія – 3, автоматизовані системи моніторингу надзвичайних ситуацій та безпека життєдіяльності – відповідно 3 кредити.

Практики також входили до складу обов'язкових компонент. Ознайомлювальна та технологічна практика уміщувала по чотири кредити, експлуатаційна та виробнича практика має 5 кредитів, підготовка та захист атестаційної роботи закладають в основу 8 кредитів. Так, загальний обсяг обов'язкових компонент складає 172 кредити.

Обсяг навчальної дисципліни вільного вибору студента, яка розміщена в Каталозі, становить 3 кредити ЄКТС. Серед них 90 годин аудиторних, що складає 30% і становить 2 години в тиждень. Обсяг вибіркових дисциплін може мати більшу кількість кредитів і у навчальних планах випускових кафедр бути з визначенням кількості кредитів та аудиторних годин в тиждень.

Для здобувачів ступеня бакалавра вибіркова частина навчального плану становить не менше 1800 годин (60 кредитів), з яких:

– частка професійно-орієнтованих вибіркових дисциплін складає 15% – не менше 36 кредитів;

– частка вибіркових дисциплін гуманітарної, фундаментальної підготовки складає 5% – не менше 12 кредитів;

– частка вибіркових дисциплін інших спеціалізацій в т.ч. іншого закладу складає 5% – не менше 12 кредитів.

Для розробки та поновлення переліку вибіркових дисциплін на початку другого семестру кожного навчального року на факультетах створюються робочі групи за головуванням деканів. Склад робочих груп затверджується наказом ректора. Робочі групи аналізують якість навчально-методичного та інформаційного забезпечення поданих дисциплін та формують свої рекомендації щодо кількісних змін у існуючому переліку дисциплін. На підставі аналізу зазначеної вище інформації робочі групи у визначені терміни формується перелік вибіркових дисциплін та передається його до інформаційного відділу для формування оновленого загально академічного каталогу, який затверджується вченою радою університету. Затверджений в установленому порядку каталог вибіркових дисциплін, рекомендованих для вивчення у наступному навчальному році, розміщується для ознайомлення здобувачів вищої освіти на офіційному сайті університету.

Загальна кількість вибіркових компонентів освітньої програми 18. До них відносяться економіка (3 кредити), соціологія, політологія (3 кредити), іноземна мова за професійним спрямуванням (5 кредитів), технічна графіка (3 кредити), створення та обробка баз даних (4 кредити), основи інформаційної безпеки держави (3

кредити), цифрова обробка сигналів (3 кредити), організаційне забезпечення технічного захисту інформації (4 кредити), технічні засоби охорони об'єктів (6 кредитів), методи та засоби захисту інформації (5 кредитів), метрологія та вимірювання (3 кредити), програмування механізмів інформаційної безпеки (4 кредити), кібербезпека інфокомунікацій (4 кредити), основи комп'ютерної стеганографії (4 кредити), Системи банківської безпеки (3 кредитів), аудит інформаційної безпеки (3 кредити), компонентна база засобів технічного захисту інформації (3 кредити), безпека технологій електронного документообігу (3 кредити). Так, загальний обсяг вибіркових компонент складає 68 кредитів. Загальний обсяг освітньої програми складає 240 кредитів.

Атестація випускників освітньої програми спеціальності 125 Кібербезпека проводиться у формі захисту кваліфікаційної роботи та завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації – бакалавр з кібербезпеки. Атестація здійснюється відкрито і публічно [8].

До програмних результатів навчання відносяться базові знання фундаментальних наук, в обсязі, необхідному для освоєння загальнопрофесійних дисциплін, знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації. Значущими є знання функціонування інформаційно-технологічних систем та мереж і їхніх компонентів законодавчої та нормативно-правової бази, а також вимог відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.

Також до програмних результатів віднесено знання з проектування та розробки систем, технологій і засобів інформаційної

безпеки та уміння оцінювати стан інформаційної безпеки об’єктів і систем, знання сучасних технічних і програмно-апаратних засобів захисту обробки інформації в інформаційно-технологічних системах. Актуальними є базові знання методів протидії несанкціонованому проникненню в інформаційно-телекомунікаційних системи і мережі; в галузі сучасних інформаційних технологій; знання з проектування комплексної системи захисту інформації інформаційно-технологічних систем та з криптографіческих методів захисту інформації, знання з організаційного забезпечення технічного захисту інформації на об’єктах інформаційної діяльності [1].

Досягнутими результатами також вважаються здатність удосконалювати і розвивати свій інтелектуальний і загальнокультурний рівень, самостійно навчатись новим методам дослідження, до змін наукового і науково-виробничого профілю в своїй професійній діяльності; вибір основних методів та способів захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки. Сюди також відносяться проектування та реалізація комплексної системи захисту інформації автоматизованих систем організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації.

Продуктивними наслідками навчання майбутніх фахівців з кібербезпеки також прийнято вважати здатність використовувати інструментальні засоби оцінки наявних вразливостей, застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах та вирішувати завдання захисту програм та даних інформаційно-технологічних систем програмно-апаратними засобами та давати оцінку якості

прийнятих рішень. Можливість здійснення оцінки захищеності інформаційно-технологічних систем та мереж, можливості проникнення в інформаційно-технологічні системи та мережі шляхом експлуатації наявних вразливостей також можна віднести до результатів навчання. Результативність навчання забезпечують здійснення організації робіт з технічного захисту інформації на об'єктах інформаційної діяльності, розробка та оцінювання моделі і політика безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем, прийняття участі у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації, впровадження процесів виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної кібербезпеки, а також застосування національних та міжнародних регулюючих актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки.

Висновки. Отже, зміст підготовки бакалаврів з кібербезпеки характеризується обов'язковим професійним навчанням з метою отримання бакалавром кваліфікації фахівця захисту інформації в інформаційних і комунікаційних системах та передбачає практику, з метою забезпечення умов підготовки фахівця в реальному середовищі майбутньої професійної діяльності. До програмних результатів навчання відносяться базові знання фундаментальних наук, в обсязі, необхідному для освоєння загальнопрофесійних дисциплін, знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації. Виникає потреба у базових знаннях методів протидії несанкціонованому проникненню в інформаційно-телекомунікаційних системи і мережі та у галузі сучасних інформаційних технологій. Підготовка такого фахівця

передбачає формування та розвиток професійних компетентностей щодо захисту інформації на об'єктах інформаційної діяльності; вивчення теоретичних та методичних положень, організаційних та практичних інструментів зі спеціальності кібербезпеки; методики та технології забезпечення безпеки інформації.

Література:

1. *Освітня програма зі спеціальності 125 «Кібербезпека»,* (2019).

2. О. Ткаченко та К. Ткаченко, (2018). Збереження культурної спадщини
та доступ до цифрових ресурсів, *Цифрова платформа: інформаційні технології в соціокультурній сфері, № 1*, pp. 75-86, 2018.

3. *Information systems defence and security: France's strategy,* (2011). [Онлайновий]. Available:www.gouvernement.fr/sites/default /files/fichiers joints/livreblanc-sur-la-defense-et-la- securite-nationale_ 2013.pdf/. [Дата звернення: 22. 10. 2019].

4. *Canada's Cyber Security Strategy*. (2010). [Онлайновий]. Available:
www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrtstrtgy/cbr-scrt-strtgy-eng.pdf/
[Дата звернення: 04. 05. 2019].

5.*National Cyber Security Strategies, 2012.* Practical Guide on Development
and Execution. ENIS. (2013)

6.*National Cyber Security Strategy and 2013-2014, Action Plan, Republic of Turkey*, (2013).

7.*Association for Computing Machinery, Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering* (англійською). (2016). New York: Computer Engineering Curricula.

8. *Освітньо-професійна програма,* 2016. [Онлайновий].

Available:
https://onat.edu.ua/wp-content/uploads/2018/05/%D0%9E%D0%9F%D0%9F_%D0%B1%D0%B0%D0%BA%D0%B0%D0%BB%D0%B0%D0%B2%D1%80_125.pdf.
[Дата звернення: 13. 03. 2020].

References:

1. *Osvitnia prohrama zi spetsialnosti 125 «Kiberbezpeka»,* (2019).
2. O. Tkachenko ta K. Tkachenko, (2018). *Zberezhennia kulturnoi spadshchyny ta dostup do tsyfrovykh resursiv, Tsyfrova platforma: informatsiini tekhnolohii v sotsiokulturnii sferi, № 1*, pp. 75-86
3. *Information systems defence and security: France's strategy*, 2011. [Onlainovyi]. Available: www.gouvernement.fr/sites/default /files/fichiers joints/livreblanc-sur-la-defense-et-la- securite-nationale_2013.pdf/. [Data zvernennia: 22. 10. 2019].
4. *Canada's Cyber Security Strategy,* (2010). [Onlainovyi]. Available: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrtstrtgy/cbr-scrt-strtgy-eng.pdf. [Data zvernennia: 04. 05. 2019].
5. *National Cyber Security Strategies*, 2012. Practical Guide on Development and Execution. ENISA, (2013).
6. *National Cyber Security Strategy and 2013-2014*, Action Plan, Republic of Turkey, 2013.
7. *Association for Computing Machinery, Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering* (anhliskoiu)., (2016). New York: Computer Engineering Curricula.
8. *Osvitno-profesiina prohrama*, (2016). [Onlainovyi]. Available: https://onat.edu.ua/wp-content/uploads/2018/05/%D0%9E%D0%9F%D0%9F_%D0%B1%D0%B0%D0%BA%D0%B0%D0%BB%D0%B0%D0%B2%D1%80_125.pdf.
[Data zvernennia: 13. 03. 2020].