МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
СЛУЖБА БЕЗПЕКИ УКРАЇНИ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Київський національний університет імені Тараса Шевченка
Одеська національна академія зв'язку імені О. С. Попова
Національний університет оборони України імені Івана Черняховського
Національна академія внутрішніх справ
Національна академія Служби безпеки України

На здобуття Державної премії України в галузі освіти

РЕФЕРАТ РОБОТИ «ТЕОРЕТИКО-МЕТОДОЛОГІЧНЕ ОБҐРУНТУВАННЯ І ПРАКТИЧНЕ ВПРОВАДЖЕННЯ СИСТЕМИ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ З КІБЕРБЕЗПЕКИ»

Номінація «Наукові досягнення в галузі освіти»

Київ – 2019

АВТОРСЬКИЙ КОЛЕКТИВ:

Воробієнко Петро Петрович	–	доктор технічних наук, професор, ректор Одеської національної академії зв'язку імені О. С. Попова;
Даник Юрій Григорович	–	доктор технічних наук, професор, начальник інституту інформаційних технологій, Національний університет оборони України імені Івана Черняховського;
Корнейко Олександр Васильович	–	кандидат технічних наук, професор, завідувач кафедри інформаційних технологій та кібербезпеки, навчально-науковий інститут № 1 Національної академії внутрішніх справ;
Мамченко Сергій Миколайович	–	доктор педагогічних наук, професор, директор навчально-наукового інституту інформаційної безпеки, Національна академія Служби безпеки України;
Новіков Олексій Миколайович	–	доктор технічних наук, професор, проректор з науково-педагогічної роботи, професор кафедри інформаційної безпеки за сумісництвом, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;
Оксіюк Олександр Глібович	–	доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації, факультет інформаційних технологій Київського національного університету імені Тараса Шевченка;
Руснак Іван Степанович	–	доктор військових наук, професор, професор кафедри стратегії національної безпеки та оборони України за сумісництвом, Національний університет оборони України імені Івана Черняховського;
Телелим Василь Максимович	–	доктор військових наук, професор, професор кафедри стратегії національної безпеки та оборони України, Національний університет оборони України імені Івана Черняховського.

Актуальність теми. На протязі останніх десятиліть, а особливо в останні п'ять років в умовах здійснення масштабної гібридної агресії проти України, стрімкий розвиток та масове впровадження сучасних інформаційних технологій, формування і розвиток загальнопланетарного кіберпростору призвело до формування нового спектру ризиків і загроз у сферах національної безпеки і оборони держави, які реалізуються в кіберпросторі та (або) через кіберпростір. Кіберзагрози охоплюють всі базові сфери суспільної діяльності (політичну, воєнну, безпекову, правову, економічну, енергетичну, інфраструктурну, соціальну, духовну тощо), загрозливо впливаючи на всі складові сектору безпеки і оборони України (СБОУ).

Відповідно до чинного законодавства України до складу СБОУ входять органи державної влади, військові формування, правоохоронні та розвідувальні органи, державні органи спеціального призначення тощо, що беруть участь у формуванні та реалізації завдань із забезпечення національної безпеки і оборони України. Крім того відповідно до чинного законодавства держави до складу СБОУ відносяться також громадяни та громадські об’єднання, які добровільно беруть участь у забезпеченні національної безпеки України.

Отже, хоча переважна більшість майбутніх фахівців з кібербезпеки для СБОУ після закінчення навчання у закладах вищої освіти (ЗВО) буде проходити подальшу службу в якості військовослужбовців і осіб, які мають спеціальні звання, але деяка частка таких фахівців буде працювати в якості державних службовців та цивільних фахівців в підрозділах державних органів, підприємств оборонно-промислового комплексу, в організаціях та установах державного та приватного сектору, що опікуються питаннями інформатизації, теж саме відноситься і до випускників цивільних закладів вищої освіти, частка з яких приходить на службу в структурах СБОУ, тобто також будуть брати участь в забезпеченні безпеки кіберпростору України. Крім того, безпека національного кіберпростору багато в чому залежить від загального рівня кіберосвіти населення – тобто його обізнаності в сфері безпечного користування Інтернетом та новітніми інформаційними технологіями.

Тому питання якісної підготовки фахівців з кібербезпеки для органів та формувань, що входять до складу СБОУ, а також забезпечення загальної кіберосвіти широких верств населення, є одним із пріоритетних завдань, що визначені нормативно-правовими актами України у сфері забезпечення кібербезпеки, як однієї із важливих складових сфер національної безпеки і оборони держави в умовах ведення гібридної війни проти України.

Мета і завдання роботи. ***Мета роботи*** – теоретико-методологічне обґрунтування і практичне впровадження системи підготовки фахівців в усіх сферах забезпечення кібербезпеки (кібероборони, кіберзахисту, кіберрозвідки, кіберконтррозвідки, протидії кіберзлочинності, захисту критичної інфраструктури тощо) для сектору безпеки і оборони України, а також економіки держави.

Завдання роботи передбачали:

визначення сутності, базової системи категорій та основних загроз в сферах кібернетичної та інформаційної безпеки, нормативно-правових засад, організаційних принципів та структури національної системи кібербезпеки з метою професійно-компетентнісного підходу до формування у майбутніх фахівців з кібербезпеки компетентностей та умінь необхідних для ефективного виконання ними завдань за призначенням в сучасних умовах;

дослідження сучасних підходів, закономірностей, методів і технологій щодо теорії і практики підготовки до протидії та ведення війни у кібернетичному та інформаційному просторах, протидії кіберзлочинності тощо;

вивчення зарубіжного досвіду побудови систем забезпечення кібербезпеки та підготовки фахівців з цих питань з метою аналізу національних можливостей щодо формування незалежної соціально-детермінованої цілісної і динамічної системи підготовки фахівців з кібербезпеки для сил оборони та безпеки;

підготовка за результатами зазначених досліджень відповідних освітніх (освітньо-професійних) програм, навчальних планів, робочих програм навчальних дисциплін, наукових праць, підручників, навчальних та методичних посібників тощо для науково-методичного забезпечення освітнього процесу з підготовки, перепідготовки та підвищення кваліфікації фахівців з кібербезпеки;

обґрунтування концептуальних підходів щодо розробки функціонально-організаційної моделі загальнодержавної системи підготовки фахівців з кібербезпеки в інтересах СБОУ та загальної кіберосвіченості населення;

розробка та удосконалення складових педагогічної системи підготовки в Україні фахівців з кібербезпеки з розробкою відповідних освітньо-кваліфікаційних характеристик і освітніх стандартів на основі Національної рамки кваліфікацій для підготовки військових та цивільних фахівців у цій сфері діяльності з метою формування повного та завершеного циклу підготовки кадрів для СБОУ.

Наукова новизна отриманих результатів:

науково обґрунтовано та побудовано модель єдиного освітнього простору щодо підготовки фахівців з кібербезпеки для СБОУ, а також економіки держави;

науково обґрунтовано та оптимізовано педагогічну систему підготовки фахівців з кібербезпеки всіх освітніх рівнів, спеціальностей, спеціалізацій і освітніх програм для сил оборони та безпеки з використанням ресурсного забезпечення галузевих та відомчих ЗВО із створенням елементів єдиного соціально детермінованого освітнього простору України.

Практичне значення отриманих результатів:

обґрунтовано і розроблено нормативно-правові документи, що забезпечують функціонування національної системи забезпечення кібербезпеки, сформовано управлінські вертикалі та організаційні структури, що здійснюють управління у цій сфері суб’єктів СБОУ, включно з підготовки, перепідготовки та підвищення кваліфікації фахівців з кібербезпеки для сил оборони та безпеки;

сформовано наукові школи з дослідження проблемних питань за різними сферами забезпечення кібербезпеки держави, насамперед, щодо: планування і ведення кібероборони та кіберрозвідки, відбиття кібератак та нейтралізації кіберзагроз; криптографічного та технічного захисту інформації; захисту в кіберпросторі державних інформаційних ресурсів; здійснення захисту та аудиту захищеності інформаційно-комунікаційних і технологічних систем об'єктів критичної інфраструктури держави на вразливість; відновлення сталості і надійності функціонування інформаційно-комунікаційних, технологічних систем після здійснення кібератак; здійснення контррозвідувальних заходів в кіберпросторі; попередження, протидії та розслідування кіберзлочинів тощо;

обґрунтовано, розроблено та упроваджено систему підготовки фахівців СБОУ з кібербезпеки, освітньо-кваліфікаційні та кваліфікаційні характеристики за посадами та Національною рамкою кваліфікацій України, стандарти освіти, освітні (освітньо-професійні) та наукові (науково-професійні) програми підготовки фахівців з кібербезпеки у всіх сферах її забезпечення, всіх освітніх рівнів, спеціальностей і спеціалізацій вищої освіти з метою формування завершеного циклу підготовки кадрів для СБОУ.

Презентація результатів дослідження. Розбудова та впровадження системи підготовки фахівців з кібербезпеки для СБОУ здійснювалось упродовж двох основних етапів на державному, галузевому та відомчому рівнях згідно з програмами фундаментальних і наукових робіт Міністерства оборони (МО) України, Служби безпеки України (СБУ), Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) та інших суб'єктів СБОУ в рамках науково-дослідних робіт, що виконувались в Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського», Національному університеті оборони України імені Івана Черняховського, Житомирському військовому інституті імені С. П. Корольова, Національній академії СБУ, а саме: «Розвиток системи підготовки військових кадрів з врахуванням досягнень в галузі освіти та науки, розвитку ЗС України», шифр «Система» (державний реєстраційний номер 0197U004407); «Розробка концепції та програми розвитку системи військової освіти до 2005 року», шифр «Концепція» (державний реєстраційний номер 0197U004408); «Тенденції та перспективи інноваційного розвитку системи військової освіти», шифр «Перспектива-ВО» (державний реєстраційний номер 0101U001258); «Обґрунтування перспективної системи підготовки та підвищення кваліфікації наукових і науково-педагогічних працівників для Збройних Сил України», шифр «Підготовка-В» (державний реєстраційний номер 0116U003564); «Обґрунтування створення системи стратегічних комунікацій Міністерства оборони та Збройних Сил України, як засіб протидії гібридній війні», шифр «Стратком» (державний реєстраційний номер 0117U001581); «Розроблення методичних основ науково-обґрунтованої системи підготовки спеціалістів з питань криптографічного та технічного захисту інформації», шифр «Фах» (державний реєстраційний номер 0106U003158) та ін.

У системно-історичному аспекті ***на етапі становлення системи підготовки фахівців з кібербезпеки (1992-2013 рр.)***:

проведено дослідження щодо особливостей реалізації загроз в кібернетичному та інформаційному просторах, як нової парадигми ведення сучасної війни та тероризму і злочинності, за рахунок чого відбулось усвідомлення необхідності формування разом з національною системою забезпечення кібербезпеки відповідної соціально детермінованої системи підготовки фахівців у цій сфері для сил оборони та безпеки країни в освітньому просторі України із використанням ресурсів Міністерства освіти і науки (МОН) України, МО України та інших силових структур;

обґрунтовано і запропоновано необхідні спеціальності підготовки фахівців з кібербезпеки в усіх сферах її забезпечення, здійснено розробку необхідного науково-методичного забезпечення для існуючих на той час відповідних напрямів і спеціальностей підготовки фахівців (рис. 1);

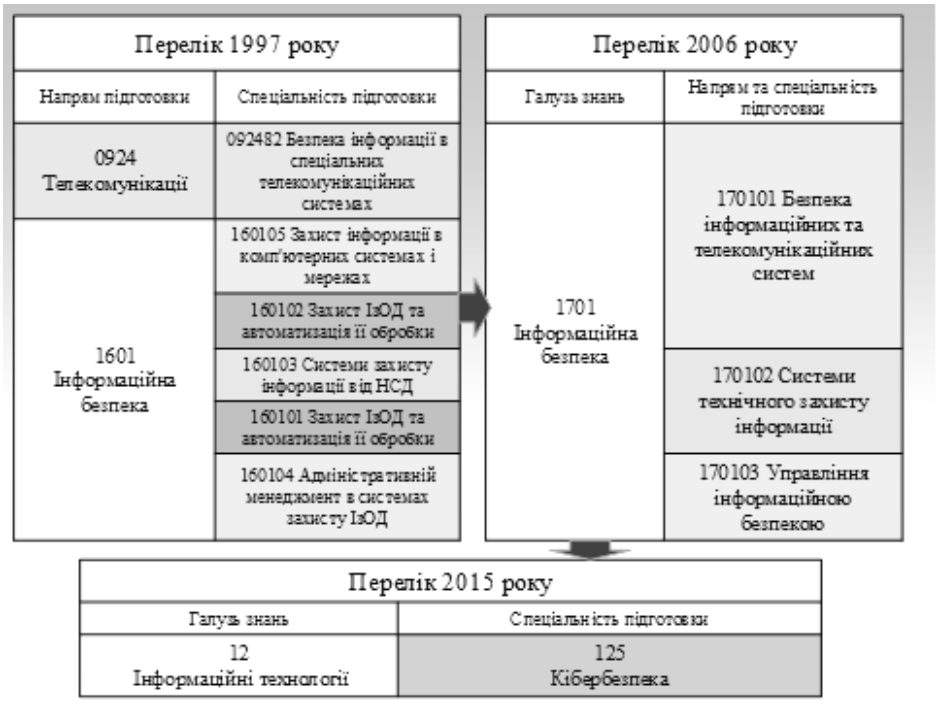

Рисунок 1 – Трансформація спеціальностей вищої освіти в сфері захисту інформації та інформаційної безпеки в сферу кібербезпеки

проведено дослідження щодо визначення фахових, соціокультурних і дидактичних чинників освіти різних категорій та фахових рівнів спеціалістів з кібербезпеки в усіх сферах її забезпечення для потреб СБОУ та економіки держави;

розроблено комплекс кваліфікаційних вимог та психологічних чинників щодо формування у курсантів, слухачів і студентів національної самосвідомості та ментально-духовних настанов щодо набуття загальних та фахових компетентностей, обґрунтування ефективних форм навчально-професійно-пізнавальної діяльності, застосування та удосконалення сучасних особистісно орієнтованих технологій підготовки фахівців з кібербезпеки в усіх сферах її забезпечення;

створено функціонально-організаційні структури педагогічної системи підготовки, перепідготовки та підвищення кваліфікації фахівців СБОУ з усіх сфер кібербезпеки, за рахунок утворення нових навчальних підрозділів або перепрофілювання існуючих, що займались підготовкою кадрів у сфері інформаційно-комунікаційних технологій та захисту інформації.

Зокрема, в інтересах забезпечення офіцерськими кадрами СБОУ в усіх сферах забезпечення кібербезпеки за активною участі членів авторського колективу створені: Інститут інформаційних технологій у складі Національного університету оборони України імені Івана Черняховського; спеціальний факультет СБУ та на його основі Інститут спеціального зв'язку та захисту інформації у складі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»; навчально-науковий інститут інформаційної безпеки у складі Національної академії СБУ; відповідні навчальні підрозділи (кафедри та факультети) в Житомирському військовому інституті імені С. П. Корольова, Національній академії внутрішніх справ тощо.

Опрацьовано штати зазначених ЗВО, методики і технології організації в них освітнього процесу, сформовано стандарти освіти, освітні (освітньо-професійні) та наукові (науково-професійні) програми підготовки фахівців з кібербезпеки усіх освітніх рівнів, спеціальностей і спеціалізацій вищої освіти, навчальних планів підготовки курсантів, слухачів і студентів усіх освітніх та кваліфікаційних рівнів підготовки (рис. 2).

Другий етап (2014-2019 рр.) – розвиток та вдосконалення системи підготовки фахівців СБОУ з кібербезпеки та забезпечення кіберосвіченості населення в умовах ведення гібридної агресії проти України. Одним із пріоритетних напрямів діяльності на цьому етапі стало вдосконалення нормативно-правової бази з питань кібербербезпеки та національної системи її забезпечення, щоб забезпечити ефективну протидію гібридній агресії проти України в кіберпросторі. Насамперед, це розроблені за участю членів авторського колективу: Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96; Закони України «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017 № 163-VIII) та «Про національну безпеку України» (від 21.06.2018 № 2469-VIII); Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.2016 № 92 та інші.

У відповідності до цих документів членами авторського колективу був зроблений вагомий внесок у: створення Державного центру кіберзахисту в системі Держспецзв'язку та відповідних ситуаційних центрів інших суб'єктів СБОУ; вдосконалення систему захищеного доступу державних органів до мережі Інтернет; здійснення участі суб'єктів СБОУ в ряді заходів щодо зміцнення міжнародного співробітництва та забезпечення поглиблення співпраці суб'єктів СБОУ з Європейським Союзом (ЄС) та НАТО для посилення спроможностей держави у сфері кібербезпеки, зокрема в рамках національної програми співробітництва Україна–НАТО.

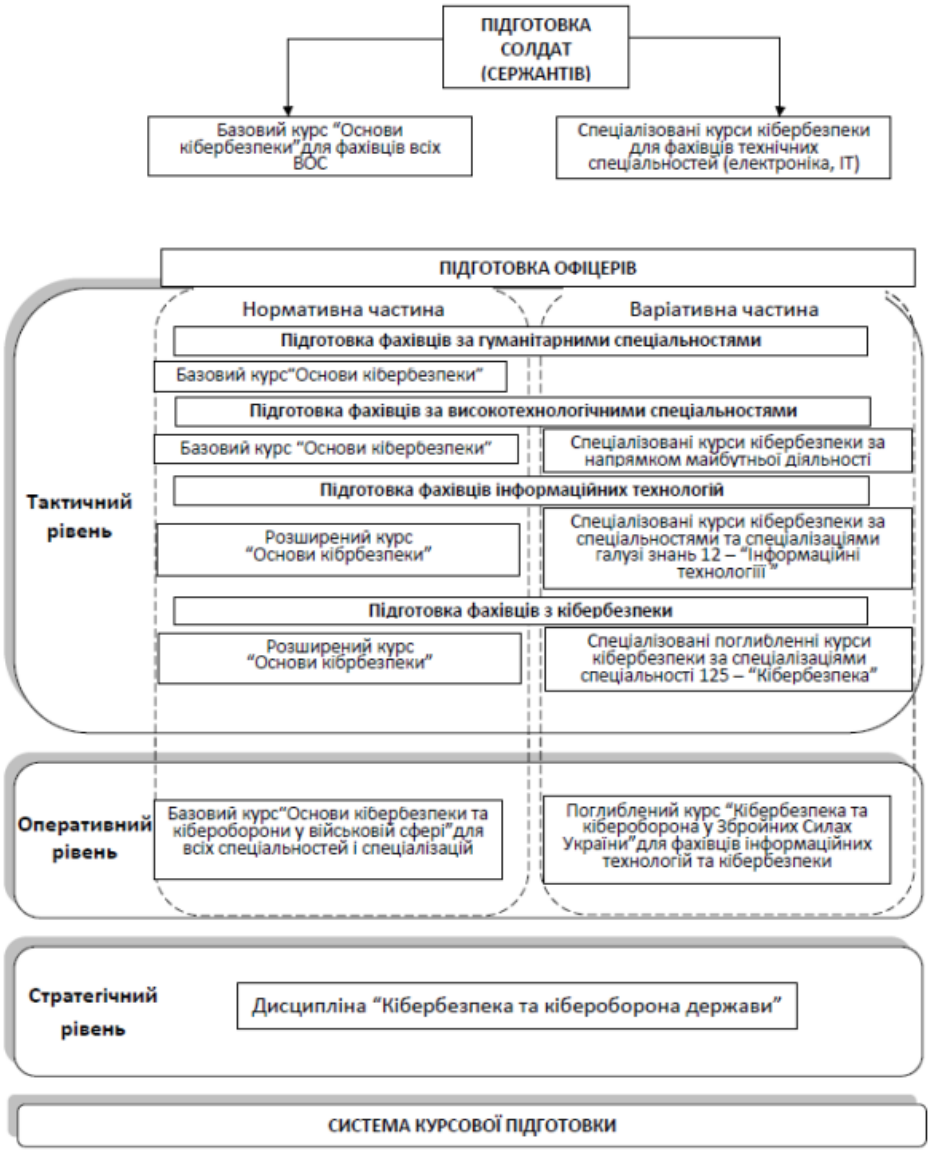

Рисунок 2 – Запропонована система навчальних курсів з кібербезпеки для військових фахівців

Для врахування зарубіжного та вітчизняного досвіду з питань забезпечення кібербезпеки та підготовки фахівців у цій сфері було організовано та проведено міжнародні та всеукраїнські конференції, семінари, формуми, засідання «за круглим столом», тренінги, навчання з питань кібербезпеки та захисту інформації в кіберпросторі.

На основі вивчення зарубіжного досвіду та цих заходів було запроваджено нову освітню спеціальність 125 «Кібербезпека» в галузі знань 12 «Інформаційні технології». Для цієї спеціальності в сфері кібербезпеки першим серед освітніх спеціальностей вищої освіти України за участю членів авторського колективу був розроблений стандарт вищої освіти для освітнього рівня бакалавр, що затверджений та введений в дію наказом МОН України від 04.10.2018 № 1074, який інтегрував в себе всі наявні здобутки та напрацювання щодо забезпечення захисту інформації, безпечного користування інформаційними технологіями, забезпечення інформаційної безпеки тощо.

Було сформовано дієву систему підготовки військових фахівців. Підготовка фахівців у сфері кібербезпеки для державних органів і формувань СБОУ ведеться в військових ЗВО (ЗВО зі специфічними умовами навчання), що підпорядковані або знаходяться в сфері управління МО України, Генерального штабу Збройних Сил України, Адміністрації Держспецзв'язку, МВС України, СБУ, розвідувальних органів України тощо.

На тактичному рівні підготовки створено умови навчання військових фахівців, які не отримують технічну освіту, для більш повного уявлення про технологічні аспекти кібербезпеки та достатнього розуміння особливостей реалізації політики кібербезпеки, як у сферах національної безпеки і оборони, так і на міжнародному рівні. При цьому фахівці з високотехнологічних напрямів отримують повні і всебічні сучасні знання з усіх сфер кібербезпеки (кібероборони, кіберзахисту, кіберрозвідки, протидії кіберзлочинам, захисту об‘єктів критичної інфраструктури тощо – за сферами компетенції ЗВО та суб'єкта СБОУ) з врахуванням кращих практик країн членів ЄС та НАТО. Основні зусилля на цьому рівні підготовки військових фахівців зосереджено на інтеграції наукового, науково-педагогічного та матеріально-технічного потенціалів на єдиній базі, шляхом формування військового ЗВО (ЗВО із специфічними умовами навчання) нового типу у вигляді інтегрованого навчально-наукового та дослідно-випробувального комплексу (інституту, академії чи університету дослідницького типу, високотехнологічних оборонних кластерів тощо).

Всі офіцери, які отримують освіту оперативного та стратегічного рівнів незалежно від галузей, спеціальностей і спеціалізацій підготовки, набувають компетентності та володіння знаннями не тільки з основ кібербезпеки у воєнній сфері, кібероборони та кіберрозвідки, але й щодо: стану та тенденцій розвитку високих та інформаційних технологій і їх застосування у сферах безпеки та оборони; інформаційно-аналітичної діяльності та імітаційного моделювання у цих сферах; організації застосування автоматизованих систем управління військами (силами) та систем типу C4ISR; організації та застосування технічних систем моніторингу (розвідки) операційного (бойового) простору в інтересах військ (сил); застосування сучасних геоінформаційних технологій та систем в інтересах військ (сил); скритого управління військами та комплексної протидії технічним розвідкам; основ захисту інформації; стратегічних комунікацій у сфері оборони тощо.

Військові фахівці, які здобули освіту цих рівнів, отримують знання та здатні практично здійснювати: формування та реалізацію державної політики з питань кібербезпеки і кібероборони; формування та реалізацію політики МО України, Збройних Сил України, інших суб’єктів СБОУ щодо дій у кіберпросторі; виконання заходів зі створення та розвитку інформаційних систем та ресурсів; координацію дій суб’єктів інформаційної- та кібер-безпеки, кібероборони та кіберрозвідки; організацію взаємодії та проведення заходів щодо підготовки держави до кібероборони зі структурними підрозділами інших центральних органів виконавчої влади та міжнародними партнерами; організовувати та підтримувати взаємодію з системою

загальнодержавної та відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT); планування та узгоджене управління діяльністю суб'єктів СБОУ у кіберпросторі за єдиним замислом і планом; моніторинг та аналіз результативності дій системи кібероборони, виявлення вразливостей в інформаційних та інформаційно-комунікаційних системах своїх і противника тощо.

Розроблено методологію побудови та функціонування цілісної системи розвитку освіченості населення України з питань кібербезпеки, яка охоплює всі рівні освіти та кваліфікації відповідно до Національної рамки кваліфікації України (рис. 3).

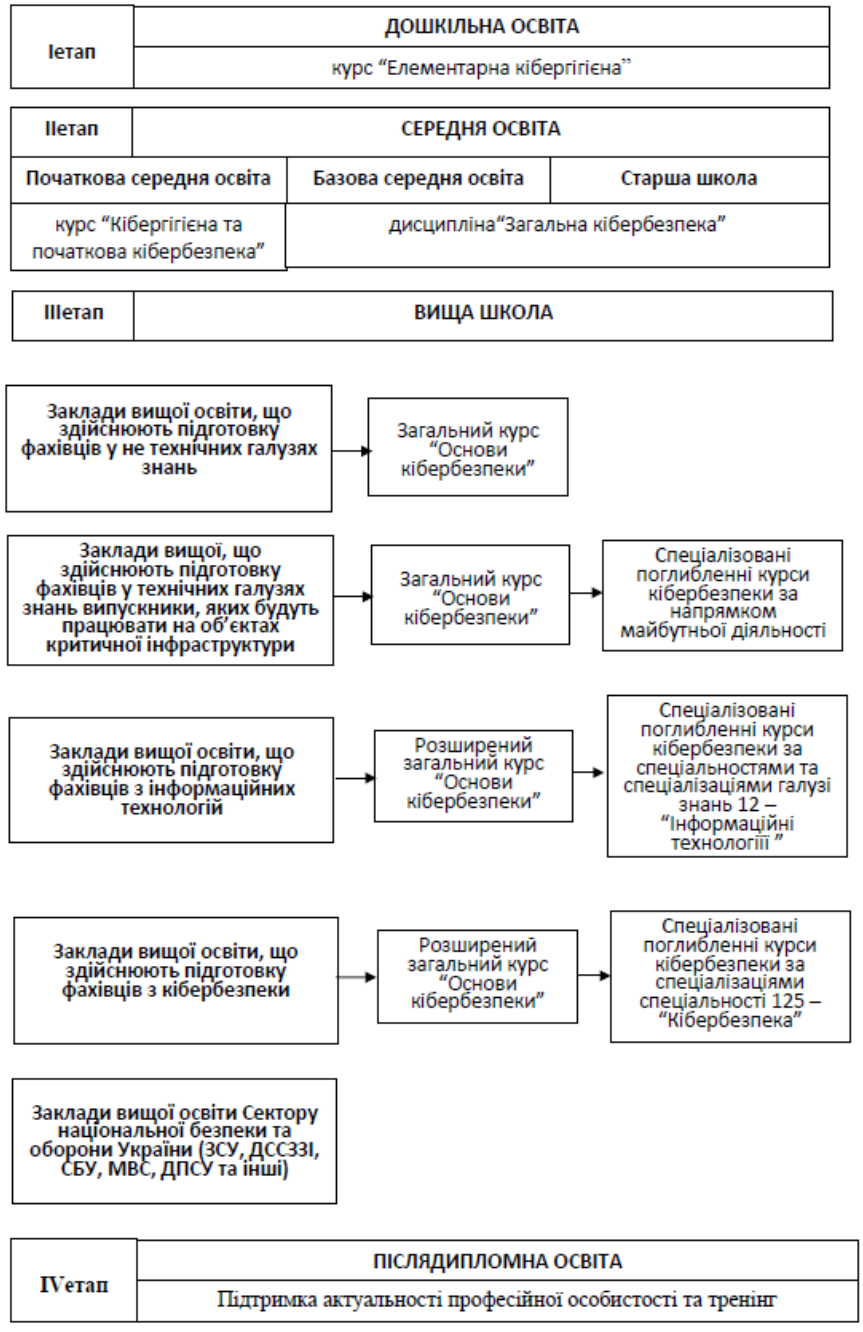

Рисунок 3 – Система розвитку освіченості населення України з питань кібербезпеки

Перший етап підготовки з кіберосвіченості населення запропоновано розпочати вже на рівні дошкільної освіти, де у дитини будуть формуватись основні базові елементи щодо кібергігієни, правильного сприйняття на рівні інстинктів меж безпеки і загроз при використанні електронних гаджетів та інших продуктів сучасних інформаційних технологій. Другим етапом підготовки з основ кібербезпеки повинна стати підготовка у шкільному віці, яку доцільно диференціювати на декілька курсів за етапами шкільної освіти: початкова освіта, базова та профільна середня освіта. Наступним, третім етапом підготовки з питань кібербезпеки, є підготовка фахівців у ЗВО, які умовно можливо розділити на групи, відповідно до галузей знань. Нарешті четвертим етапом підготовки з питань кібербезпеки є постійно діюча система курсової (післядипломної) підготовки, що виконує функції підтримуючої та тренувальної системи між розглянутими вище рівнями підготовки.

Запропонована методологія формування кіберкомпетенцій, що вже впроваджується в освітньому середовищі України, представляє собою комплексне та гнучке рішення проблемного питання освіченості суспільства та особистості з питань кібербезпеки. Вона дозволяє знизити ризики для дітей на етапі їх формування як особистості, а запровадження системи шкільної кіберосвіти надає можливість більш якісно підготувати дитину до дорослого життя, життя в сучасному високотехнологічному цифровому суспільстві. Впровадження запропонованих змін для системи вищої освіти має системний характер та підвищить конкурентну спроможність випускника на ринку праці.

За темою «Теоретико-методологічне обґрунтування і практичне впровадження системи підготовки фахівців для сектору безпеки і оборони України з кібербезпеки», за участі авторів разом:

захищено дисертаційних досліджень – 84;

підготовлено монографій, підручників – 45;

навчальних і методичних посібників, методичних вказівок – 49;

програм навчальних дисциплін та інших методичних видань – 30;

друкованих праць у наукових фахових виданнях – 241.

Висновок: цикл наукових праць, як спільне системне наукове досягнення колективу авторів у складі: Воробієнко П.П., Даник Ю.Г., Корнейко О.В., Мамченко С.М., Новіков О.М., Оксіюк О.Г., Руснак І.С., Телелим В.М. за темою: «Теоретико-методологічне обґрунтування і практичне впровадження системи підготовки фахівців для сектору безпеки і оборони України з кібербезпеки» у номінації «Наукові досягнення в галузі освіти», сприяє розвитку педагогічної науки, позитивно впливає на суспільний прогрес та інтелектуальний розвиток особистості, утверджує високий авторитет вітчизняної науки в галузі освіти через створення умов, обґрунтування та побудову моделі єдиного освітнього простору щодо підготовки фахівців для сектору безпеки і оборони України, а також економіки держави з кібербезпеки, що має важливе загальнодержавне та оборонне значення і суттєво впливає на забезпечення національної безпеки України в умовах ведення проти неї гібридної війни.

Воробієнко П.П.

Даник Ю.Г.

Корнейко О.В.

Мамченко С.М.

Новіков О.М.

Оксіюк О.Г.

Руснак І.С.

Телелим В.М.