Methods of information systems protection

УДК 004.056:378.1(477) **doi: 10.20998/2522-9052.2019.1.20**

Ю. Г. Даник[1], П. П. Воробієнко[2]

[1] Національний університет оборони України ім. Івана Черняховського, Київ, Україна
[2] Одеська національна академія зв'язку ім. О.С. Попова, Одеса, Україна

МЕТОДОЛОГІЧНІ ТА ЗМІСТОВНІ ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ КІБЕРБЕЗПЕКИ ДЛЯ ДІЙ В УМОВАХ КОМПЛЕКСНИХ КІБЕРВПЛИВІВ

Предметом дослідження є методологічні та змістовні основи з кібербезпеки та захисту інформації в телекомунікаційних системах. **Метою** статті є формування змісту та методології підготовки фахівців кібербезпеки до дій в умовах комплексних кібервпливів. **Результати.** Деструктивні кібервпливи стають все більш складними, системними і комплексними та супроводжуються ланцюговими та синергетичними ефектами. Практика доводить, що ключовим елементом для забезпечення ефективної кібербезпеки та кібероборони держави в таких умовах є наявність ефективних, адекватних, виконуваних концепцій, стратегій, планів і програм, а також організаційних заходів, сучасного якісного обладнання і особливо підготовлених фахівців у необхідній кількості. Їх наявність потребує подальшого розвитку методології їх підготовки. У статті розглянуті кібератаки на різні об'єкти критичної інфраструктури держави, а також особливості підготовки фахівців сектору безпеки і оборони тактичного рівня за високотехнологічними напрямами безпосередньо пов'язаними з застосуванням ІКТ та управління. **Висновок** зводиться до того, що запропоновані методологічні та змістовні основи освіти з питань, які є подальшим розвитком теоретичних основ і практики кіберосвіти, надають можливість поетапно та безперервно формувати і підтримувати компетентності випускників з питань кібербезпеки і кібероборони для виконання завдань за призначенням в сучасних і прогнозованих умовах.

Ключові слова: національна безпека і оборона; кіберзагрози; комплексні кібервпливи; кібербезпека; кібероборона; кіберосвіта.

Вступ

Процеси глобальної інформатизації, розвиток кібер- та інформаційних технологій призвели до того, щоб кіберінформаційна інфраструктура держав стала об'єктом різноманітних деструктивних кібервпливів. Кіберзброю за наслідками її застосування більшість фахівців асоціюють зі зброєю масового ураження [1]. Безпека держави суттєвим чином залежить від стійкості та стану об'єктів критичної інфраструктури держави, від їх захищеності, як від звичайних кібервпливів, так і від комплексних і системних розподілено-зосереджених впливів з ланцюговими ефектами [2]. Недостатня стійкість та нестабільна робота об'єктів критичної інфраструктури наносять колосальні збитки державі та населенню. Наприклад, відключення електроенергії в результаті здійснення кібервпливів з великою ймовірністю може призвести як до значних економічних втрат, так і до хаосу у великих містах. Такі кіберзагрози можуть бути реалізовані шляхом впливу як на весь енергетичний комплекс в цілому, так і на окремі його або пов'язані з ним елементи. Вплив може проводитись комплексно, одночасно, послідовно або змішано. Протягом 2014-2018 років об'єкти критичної інфраструктури держави неодноразово піддавалися різноманітним комплексним деструктивним кібервпливам.

Збої у функціонуванні транспортної, телекомунікаційної, фінансової систем, системи життєзабезпечення, безпеки населення можуть призвести до глобальних екологічних та техногенних наслідків. Усі галузі та об'єкти в сучасних умовах пов'язані між собою, тобто створений так званий «ланцюг». Виведення з ладу або порушення функціонування критичних елементів взаємопов'язаних систем, як правило, призводить до ланцюгових ефектів розповсюдження збоїв і порушень, наслідком яких можуть стати надзвичайні ситуації, аварії, катастрофи тощо [2]. Проблема забезпечення кібербезпеки та кібероборони держави постійно ускладнюється і є надважливою для забезпечення безпеки і оборони держави, її економічного та соціального розвитку, і потребує системних, комплексних підходів для свого вирішення. Для протидії таким кібервпливам, що несуть в собі найбільш важкі наслідки для населення та держави в цілому, необхідно мати відповідно підготовлених фахівців [3, 4] .

Аналіз досліджень і публікацій. Журнал Cyber Education, що видається Cyber Innovation Center USA, констатує: "Сьогодні наша країна наражається на нестачу робітників у сфері кібербезпеки. Фактично, на даний час у нас більш 380 000 робочих місць у сфері кібербезпеки. Їх кількість зросте до 1 мільйона у 2020 році. Нестача кваліфікованих фахівців у галузі кібербезпеки представляє великий ризик не тільки для національній безпеки нашої країни, але і для нашої економічної безпеки".

Найбільш інтенсивно в цій сфері діють КНР, Ізраїль, Японія, РФ, США та країни-члени НАТО. Питання кіберосвіти є невід'ємною складовою забезпечення кібербезпеки і кібероборони будь-якої держави [5–14].Але, як свідчить проведений аналіз відомих публікацій, єдина базова методологія та зміст навчання з питань підготовки фахівців у галузі кібербезпеки і загальної кіберосвіти так само, як термінологія, загальновизнана і загальноприйнята система стандартів у цій галузі досі не сформувалися [2]. Тому **метою статті** є формування змісту та методології підготовки фахівців кібербезпеки до дій в умовах комплексних кібервпливів.

Виклад основного матеріалу

Для реалізації комплексного і гнучкого підходу до підготовки фахівців кібербезпеки і кібероборони, здатних ефективно діяти в умовах комплексних деструктивних кібервпливів, на основі методів індукції та дедукції, системного аналізу та аналогій, віртуальної реальності, інформаційного моделювання та інформаційного підходу, дослідження формування самоосвітньої компетентності та фахових, психолого-педагогічних і дидактичних чинників освіти була розроблена та апробована система їх підготовки, а також зміст навчання із загальної кіберосвіти у непрофільних закладах вищої освіти [5].

З цією метою запропоновано здійснення розподілу на підготовку фахівців за високотехнологічними напрямами та підготовку всіх інших фахівців. Таким чином, створюються умови щоб фахівці, які не мають технічної освіти, отримали більш повне уявлення про технологічні аспекти кібербезпеки і у достатній мірі розумілися щодо особливостей реалізації політики кібербезпеки як у сфері оборони держави, так і на міжнародному рівні, а фахівці з високотехнологічних напрямів отримали повні і всебічні сучасні знання з питань кібербезпеки і кібероборони, їх організації і управління ними із врахуванням кращих практик країн-членів НАТО.

Розглянемо особливості підготовки фахівців сектору безпеки і оборони тактичного рівня за високотехнологічними напрямами безпосередньо пов’язаними з застосуванням ІКТ та управління. Для цих спеціальностей і спеціалізацій доцільно ввести у нормативну частину базовий курс з питань кібербезпеки та у варіативну частину спеціалізовані курси за складовими кібербезпеки, які охоплюють питання загальної, соціальної, технічної та військової кібернетики, кіберпростір та його особливості, загрози і ризики у кібернетичній сфері; основи інформаційної кібербезпеки і кібероборони, технологічні, соціотехнічні, інформаційні та інші аспекти кібербезпеки і кібероборони; особливості організації та стандарти у сфері кібербезпеки і кібероборони у світі та в Україні; управління кібербезпекою в сфері національної безпеки та оборони. Особливу увагу слід приділити захисту інформації в телекомунікаційних системах (ТКС) як найбільш привабливого об’єкта для комплексних кібервпливів. Для комплексного вирішення задачі кіберзахисту ТКС використовують еталонну модель відкритих систем (МВС), яка розроблена Міжнародною організацією із стандартизації (МОС) в 1984 році. Ця модель відіграла виключну роль в побудові глобальної інформаційної інфраструктури. З розвитком технологій модель ВОС вже не змогла вирішувати нових задач у зв’язку з багатофункціональністю процесів, які відбуваються в мережі. В 2001 році була запропонована узагальнена модель ВОС, де крім рівнів введено площини (підплощини) за їх функціональним призначенням [6]. Таких площин на початку було 7, а напів-площин – 11. Назвемо декілька площин: Користувача, Маршрутизації, Сигналізації, Управління, Синхронізації. В кожну площину доцільно ввести напів-площину, яка забезпечить кіберзахист процесів за їх функціональним призначенням: передача інформації користувачеві, встановлення з’єднання (маршрутизація, сигналізація), синхронізація роботи пристроїв, забезпечення якості послуг та інше.

Кіберзахист ТКС можливо відносно легко систематизувати, тому що в [7] наведена математична модель телекомунікаційних систем.

Слід також вказати на майбутні ризики та загрози, які пов’язані з майбутнім впровадженням квантових комп’ютерів та хмарних обчислень. Запобіжником цих загроз є квантовий захист інформації, постквантова криптографія тощо [8, 9, 15].

Методичні основи та практика проведення аналізу загроз, ризиків і уразливостей є базовими для формування навичок розробки стратегії та архітектури кібербезпеки, запобігання, обмеження та нейтралізації відомих і невідомих уразливостей та загроз, управління кібернетичними ризиками з метою їх зниження. Огляд уразливостей, характерних для кіберпростору, форм, способів, засобів використання таких уразливостей, основний спектр різноманітних сценаріїв та технологій кіберрозвідки, кіберзахисту або активного впливу (несанкціонованого проникнення, отримання інформації, зміни алгоритмів діяльності тощо) сформує у тих, хто навчається, вміння оцінювати ризики деструктивних впливів, в тому числі і пов'язаних з використанням мобільних приладів (гаджетів), інших технологій і систем, що пов’язані з мобільністю.

Важливою складовою підготовки фахівців з питань кібербезпеки є вивчення ними світового і вітчизняного досвіду створення і розвитку систем кібербезпеки та їх складових; вирішення питань забезпечення кібербезпеки на різних етапах її становлення; розподілу сфер відповідальності, задач, функцій, організації взаємодії з питань кібербезпеки і кібероборони між складовими національної безпеки та оборони; міжнародних та національних стандартів у галузі кібербезпеки; особливості формування національної політики з кібербезпеки, найкращих світових практик у вирішенні зазначених питань та тенденцій їх розвитку; загальної системи та структури міжнародних і національних організацій у сфері кібербезпеки, їх завдання, організаційна структура, повноваження, задачі, функції, розподіл повноважень між ними; організація та характер взаємодії з національними організаціями з кібербезпеки; міжнародні та національні правові аспекти забезпечення кібербезпеки та відповідальності за здійснення деструктивних впливів у кібернетичному просторі та їх наслідки, основ медіакультури (знань та вмінь здійснення соціальних комунікацій в електронному медіасередовищі).

Підготовка фахівців за високотехнологічними напрямами, фахівців кібербезпеки та всіх інших військових фахівців з вищенаведених базових питань кібербезпеки відрізняється лише шириною та глибиною їх подання, але охоплює їх всі без винятку.

Компетентності з питань кібербезпеки, необхідні для виконання завдань за посадами випускниками військових ЗВО – фахівцями з кібербезпеки,

будуть закладатися при вивченні управління кібербезпекою у сфері національної безпеки і оборони у рамках варіативних дисциплін. На основі попередньо засвоєних базових знань з кібербезпеки здійснюється їх підготовка до виконання завдань за посадою командира підрозділу військової частини кібербезпеки або офіцера з кібербезпеки органу військового управління. Для цього вони вивчають основні кіберзагрози у сфері національної безпеки і оборони, відомчі нормативні акти з кібербезпеки і кібероборони, зміст, завдання та складові частин кібероборони, сили та засоби кібероборони, форми і способи бойового застосування підрозділів кібервійськ та вимоги до їх спроможностей, досвід їх підготовки і застосування. Крім цього, вивчають досвід провідних країн світу, методи роботи посадових осіб та методики планування застосування підрозділів кібернетичного захисту у мирний час і в особливий період, усвідомлюють розподіл повноважень з питань кібербезпеки і кібероборони між суб'єктами забезпечення кібербезпеки, засвоюють особливості підготовки і проведення навчань з кібероборони, аудиту та оцінки кібербезпеки на рівні військової частини та органу військового управління.

Особливу увагу слід приділяти практичній складовій підготовки на розробленому, наближеному до реального, тактичному або оперативному фоні із використанням кіберполігонів та засобів дистанційного проведення кібернавчань. Подальше нарощування циклу розглянутих питань надасть можливість сформувати зміст навчання для підготовки фахівця з кібербезпеки тактичного рівня з необхідними компетенціями.

Аналіз стандартів підготовки фахівців тактичного рівня Сектору національної безпеки і оборони України СНБОУ всіх галузей знань (крім високотехнологічних спеціальностей та спеціалізацій) виявив наявність компетенцій щодо застосування ІКТ за профілем діяльності та відсутність системних компетенцій випускника з питань кібербезпеки і кібероборони. Доцільно доповнити нормативну частину навчання базовим курсом (дисципліною, блоком у дисципліні) основ кібербезпеки з урахуванням подальшого посадового призначення випускника. Змістом навчання будуть такі питання: загальна і військова кібернетика, кіберпростір та його особливості, загрози і ризики у кібернетичній сфері, основи інформаційної, кібербезпеки і кібероборони, технологічні, соціо-технічні, інформаційні та інші аспекти кібербезпеки і кібероборони, основні заходи кіберзахисту під час виконання обов'язків за посадою.

Фахівці з кібербезпеки та кібероборони, які отримали освіту цих рівнів, повинні отримати знання та бути здатними практично здійснювати: формування та реалізацію державної політики з питань інформаційної, кібербезпеки та кібероборони; формування та реалізацію політики Міністерства оборони (МО) України та Збройних Сил (ЗС) України щодо дій у кіберпросторі; виконання заходів зі створення та розвитку інформаційних систем та ресурсів у ЗС України; координацію дій суб'єктів інформаційної, кібербезпеки та кібероборони МО та ЗС України; розробку стандартів підготовки фахівців з інформаційної, кібербезпеки та кібероборони; організацію взаємодії та проведення заходів (в т.ч. щодо підготовки держави до кібероборони) зі структурними підрозділами інших центральних органів виконавчої влади та міжнародними партнерами; організовувати та підтримувати взаємодію з системою відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT); планування та узгоджене управління діяльністю суб'єктів у кіберпросторі за єдиним замислом і планом, контроль та координацію їх дій; моніторинг та аналіз кіберінцидентів, деструктивних інформаційних та когнітивних дій у кіберпросторі; ефективності дій системи кібербезпеки і кібероборони, виявлення уразливостей в інформаційних та кібернетичних системах своїх і противника; планування, організацію та координацію розвідувальних (Cyber Warfare Intelligence), оборонних (Defensive Cyber Warfare) і наступальних (Offensive Cyber Warfare) операцій в кіберпросторі (Cyberspace Operation) та кібероперацій (Cyber Operation); організацію та координацію кібернетичних, електронних, мережевих, інформаційних, когнітивних і психологічних дій у кіберпросторі (включаючи соціальні мережі).

Особливістю підготовки фахівців оперативного рівня на цей час, у тому числі фахівців з кібербезпеки, які закінчили військові ЗВО за галуззю знань 12 "Інформаційні технології" та спеціальністю 125 Кібербезпека", є їх підготовка у межах галузі знань 25 "Воєнні науки, національна безпека, безпека державного кордону". Спеціальність "Кібербезпека" у цій галузі знань відсутня. Найбільш споріднена підготовка проводиться за спеціалізацією "Управління інформаційною безпекою у військовій сфері" у межах спеціальності 254 – "Забезпечення військ (сил)", де проводиться підготовка всіх спеціалізацій за напрямком ІТ. Такий підхід не є раціональним для формування фахівця ІТ оперативного рівня. Вважається за доцільне інтегрувати підготовку у межах окремої спеціальності з подальшим поділом на спеціалізації.

Аналіз професійних стандартів та освітньо-професійних програм усіх спеціальностей та спеціалізацій офіцера оперативно рівня показав наявність компетенції з володіння інформаційними технологіями під час вирішення професійних завдань. При цьому, у компетенціях, відсутнє згадування питань кібербезпеки і кібероборони. В сучасних умовах таке нехтування питаннями кібербезпеки і кібероборони не є прийнятним та потребує виправлення. Це викликає необхідність введення базового курсу основ кібербезпеки і кібероборони у військовій сфері для всіх спеціальностей та поглиблений курс для фахівців ІТ і кібербезпеки.

Для фахівців ІТ та кібербезпеки доцільно запропонувати поглиблений курс кібербезпеки у сфері безпеки і оборони за спеціалізаціями з урахуванням подальшого посадового призначення. Змістом навчання буде: вивчення міжнародних та відомчих стандартів у сфері кібербезпеки і кібероборони; зміст, завдання, форми організації кібероборони

держави; критична кібер- та інформаційна інфраструктура держави; структура і принципи управління глобальною мережею Інтернет, телекомунікаційними мережами, соціальними мережами; склад сил і засобів кібербезпеки та кібероборони держави, їх завдання, можливості; основи підготовки і ведення кібероборони держави та кібернетичної операції Збройних Сил України; форми та способи застосування військових частин і підрозділів кібербезпеки під час здійснення кібероборони держави, кібернетичної та інших операцій Збройних Сил України і угруповань військ; методи роботи посадових осіб з кібербезпеки органів військового управління, командирів військових частин та установ кібербезпеки під час виконання завдань у мирний час, в особливий період і за воєнного стану.

Висновки

Деструктивні кібервпливи стають все більш складними, системними і комплексними та супроводжуються ланцюговими та синергетичними ефектами. Практика доводить, що ключовим елементом для забезпечення ефективної кібербезпеки та кібероборони держави в таких умовах є наявність ефективних, адекватних, виконуваних концепцій, стратегій, планів і програм, а також організаційних заходів, сучасного якісного обладнання і особливо підготовлених фахівців у необхідній кількості. Їх наявність потребує подальшого розвитку методології їх підготовки. Слід зазначити, що кібербезпека вже кваліфікується як самостійний напрям фундаментальних наук, який поєднує в собі, як природньонаукові, так і гуманітарні аспекти, а використання її методів дозволяє отримувати принципово нові фундаментальні знання.

Запропоновані методологічні та змістовні основи освіти з питань кібербезпеки та система для підготовки фахівців СНБОУ які є подальшим розвитком теоретичних основ і практики кіберосвіти надають можливість поетапно та безперервно формувати і підтримувати компетентності випускників з питань кібербезпеки і кібероборони для виконання завдань за призначенням в сучасних і прогнозованих, перспективних умовах.

Список літератури

1. Присяжнюк М. М., Цифра Є. І. Особливості забезпечення кібербезпеки. *Реєстрація, зберігання та обробка даних*, 2017. Т. 19, № 2. С. 61–68.
2. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
3. Діордиця І. Кваліфікаційні вимоги до фахівців із кібербезпеки. *Підприємництво, господарство і право*. 2017. № 2. С. 215–219.
4. Бистрова Б. В. Особливості формування системи професійної підготовки бакалаврів з кібербезпеки у ВНЗ США. *Вісник Черкаського університету*. 2017. № 6. С. 15–18.
5. Даник Ю. Г., Телелим В. М., Радецький В. Г. Питання трансформації оборонних структур держави та удосконалення системи військової освіти. *Наука і оборона*. 2009. №1. С. 15–16.
6. Воробиенко П. П. Концепция обобщенной эталонной модели взаимодействия открытых систем. *Электросвязь*. 2001. № 10. С. 14-15.
7. Воробиенко П. П., Струкало М. И. Обобщенная математическая модель взаимодействия телекоммуникационных систем. *Электросвязь*. 2003. № 11. С.44-46.
8. Кучук Г.А. Метод оценки характеристик АТМ-трафика. *Інформаційно-керуючі системи на залізничному транспорті*. 2003. .№ 6. .С. 44-48.
9. Amin Salih M., Yuvaraj D., Sivaram M., Porkodi V. Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol. *International Journal of Advanced Research in Computer Science*. Vol. 9, No 6. P. 1–6, DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335
10. Amin Salih M., Potrus M.Y. A Method for Compensation of TCP Throughput Degrading During Movement Of Mobile Node. *ZANCO Journal of Pure and Applied Sciences*. Vol. 27, No 6. P. 59-68.
11. Saravanan S., Hailu M., Gouse G.M., Lavanya M., Vijaysai R. Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip. International Conference on Advances of Science and Technology, ICAST 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Vol. 274. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-15357-1_34
12. Коваленко А.А., Кучук Г.А. Сучасний стан та тенденції розвитку комп'ютерних систем об'єктів критичного застосування. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2018. Вип. 1(47). С. 110–113.
13. Кучук Г.А., Можаєв О.О., Воробйов О.В. Метод агрегування фрактального трафіка. *Радіоелектронні та комп'ютерні системи*. 2006. № 6 (18). С. 181–188.
14. Porkodi V., Sivaram M., Mohammed A.S., Manikandan V. Survey on White-Box Attacks and Solutions. Asian Journal of Computer Science and Technology. Vol. 7, Is. 3. pp. 28–32.
15. Горбенко Ю. І., Ганзя Р. С. Аналіз стійкості постквантових криптосистем. *Прикладная электроника*. 2014. Т. 13, № 3. С. 268–274.

References

1. Prysyazhnyuk, M. M. and Tsifra, E. I. (2017), “Features of providing cyber security”, *Registration, storage and processing of data*, Vol. 19, No. 2, pp. 61–68.
2. Danik, Yu. G. and Grischuk, R. V. (2016), *Fundamentals of Cybernetic Security*, ZNAMEU, Zhytomyr, 636 p.
3. Dioritsa, I. (2017), “Qualification Requirements for Cybersecurity Specialists”, *Entrepreneurship, Economy and Law*, No. 2, pp. 215-219.
4. Bystrov, B. V. (2017), “Features of the formation of the system of professional training of bachelors of cyber security in US universities”, *Herald of Cherkasy University*, No. 6, pp. 15–18.

5. Danik, Yu. G., Teleim, V. M. and Radetsky, V.G. (2009), “The Problems of Transformation of State Defense Structures and Improvement of the System of Military Education”, *Science and defense*, No. 1, pp. 15–16.
6. Vorobiyenko, P. P. (2001), “Concept of the generalized reference model of the interaction of open systems”, *Electrosvyaz*, No. 10, pp. 14–15.
7. Vorobiyenko, P. P. and Strukalo, M. I. (2003), “A Generalized Mathematical Model for the Interaction of Telecommunication Systems”, *Electrosvyaz*, No. 11. pp. 44–46.
8. Kuchuk, G.A. (2003), "Method of estimation of characteristics of ATM traffic", *Information and control systems in the railway transport*, No. 6, pp. 44-48.
9. Amin Salih, M., Yuvaraj, D., Sivaram, M. and Porkodi, V. (2018), “Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol”, *International Journal of Advanced Research in Computer Science*, Vol. 9, No 6, pp. 1–6, DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335
10. Amin Salih M. and Potrus M.Y. (2015), “A Method for Compensation of Tcp Throughput Degrading During Movement Of Mobile Node”, *ZANCO Journal of Pure and Applied Sciences*, Vol. 27, No 6, pp. 59-68.
11. Saravanan, S., Hailu, M., Gouse, G.M., Lavanya, M. and Vijaysai, R. (2019), “Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip”, *International Conference on Advances of Science and Technology*, ICAST 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol 274, Springer, Cham, DOI: https://doi.org/10.1007/978-3-030-15357-1_34
12. Kovalenko, A.A. and Kuchuk, G.A. (2018), “The current state and trends of the development of computer systems of objects of critical application”, *Systems of control, navigation and communication*, PNTU, Poltava, No. 1 (47), pp. 110–113.
13. Kuchuk, G.A., Mozhaev, O.O. and Vorobyov, O.V. (2006), “The method of aggregation of fractal traffic”, *Radioelectronic and computer systems*, No. 6 (18), pp. 181–188.
14. Porkodi, V., Sivaram, M., Mohammed, A.S. and Manikandan, V. (2018), “Survey on White-Box Attacks and Solutions”, *Asian Journal of Computer Science and Technology*, Vol. 7, Issue 3, 2018, pp. 28–32.
15. Gorbenko, Yu. I. and Hansa, R. S. (2014), “Analysis of stability of post-quantum cryptosystems”, *Applied electronics*, Vol. 13, No. 3, pp. 268–274.

Received (Надійшла) 29.01.2019
Accepted for publication (Прийнята до друку) 20.03.2019

Методологические и содержательные особенности подготовки специалистов для действий в условиях комплексных кибервоздействий

Ю. Г. Данык, П. П. Воробиенко

Предметом исследования является методологические и содержательные основы по кибербезопасности и защиты информации в телекоммуникационных системах. **Целью** статьи является формирование содержания и методологии подготовки специалистов по кибербезопасности к действиям в условиях комплексных кибервлияний. **Результаты**. Деструктивные кибервлияния становятся все более сложными, системными и комплексными и сопровождаются цепными и синергетическими эффектами. Практика показывает, что ключевым элементом для обеспечения эффективной кибербезопасности и кибероборони государства в таких условиях является наличие эффективных, адекватных, выполняемых концепций, стратегий, планов и программ, а также организационных мероприятий, современного качественного оборудования и особенно подготовленных специалистов в необходимом количестве. Их наличие требует дальнейшего развития методологии их подготовки. В статье рассмотрены кибератаки на различные объекты критической инфраструктуры государства, а также особенности подготовки специалистов сектора безопасности и обороны тактического уровня за высокотехнологичными направлениями, непосредственно связанными с применением ИКТ и систем управления. **Вывод** сводится к тому, что предложенные методологические и содержательные основы образования по вопросам кибербезопасности, которые являются дальнейшим развитием теоретических основ и практики киберобразования, предоставляют возможность поэтапно и непрерывно формировать и поддерживать компетентности выпускников по вопросам кибербезопасности и кибероборони для выполнения задач по назначению в современных и прогнозируемых условиях.

Ключевые слова: национальная безопасность и оборона; киберопасность; комплексные кибервлияния; кибербезопасность; кибероборона; киберобразование.

Methodological and substantive features of training specialists for actions in conditions complex cyber influences

Yu. Danyk, P. Vorobiyenko

The subject of the study is the methodological and substantive basis of telecommunication systems cybersecurity and information security. **The purpose** of the article is to formulate the content and methodology of training specialists in cybersecurity to operate under conditions of complex cyber factors. **Results**. Destructive cyber-impacts become more complex, systemic and complex, and are accompanied by chain and synergistic effects. Practice proves that the key to effective cyber security and the state's cyber defense is the availability of effective, adequate, implemented concepts, strategies, plans and programs, as well as organizational measures, modern high-quality equipment and especially trained specialists in the required quantity. Their presence needs further development of the methodology of their preparation. The article deals with cyber attacks on various objects of critical state infrastructure, as well as personnel specific training in the security sector and tactical level defense in high-tech areas directly related to the use of ICTs and management systems. **The conclusion** is that the proposed methodological and substantive foundations of cybersecurity education, which are the further development of the theoretical foundations and practices of cyber education, provide the opportunity to gradual and continuous development and maintain the competence of cybersecurity and cyber defense graduates to perform assignments under current and expected conditions.

Keywords: national security and defense; cyber threats; integrated cyber attacks; cyber security; cyber defense; cyber education.