Живило Євген Олександрович,
аспірант кафедри інформаційних технологій і систем управління,
Харківський регіональний інститут державного управління
Національної академії державного управління при Президентові України,
м. Харків
ORCID 0000-0003-4077-7853

УДК 351.865 **doi: 10.34213/tp.19.02.32**

СУТНІСТЬ ОСНОВНИХ ЗАВДАНЬ СИСТЕМИ КІБЕРОБОРОНИ УКРАЇНИ

Проаналізовано сутність сучасних напрямів створення та функціонування системи кібероборони держави. Визначено, що для сучасної України успішний перехід до реалізації заходів із підготовки та ведення кібероборони можливий лише за умови попереднього визначення напрямів і завдань функціонування системи кібероборони.
Сформульовано висновки щодо ролі нинішнього політико-правового курсу функціонування системи кібероборони, сформовано подальші вимоги до набуття спроможностей сектору безпеки і оборони держави в системі кібероборони України на основі найкращих практик держав – членів ЄС та країн – членів НАТО.
Ключові слова: кібероборона держави, спроможності сектору безпеки і оборони держави, кіберпростір, кіберзагрози, кіберзахист критичної інформаційної інфраструктури.

Актуальність створення та функціонування системи кібероборони держави. Прогноз розвитку безпекового середовища навколо України свідчить, що успішна побудова системи кібероборони нездійснена в межах чинної системи державного управління. Дійовий єдиний підхід у секторі безпеки держави щодо реалізації заходів із підготовки та ведення кібероборони здійснено в межах чинної, успадкованої від радянського і ще більш далекого минулого системи державного управління.

Поступова трансформація системи кібероборони в одну із сучасних європейських моделей здається принципово неможливою, оскільки ґрунтуються вони на різних політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших засадах. Пошук нормативної моделі системи кібероборони, адекватної умовам управління пострадянських країн, є завданням вкрай актуальним і своєчасним.

У новітньому варіанті створення та функціонування системи кібероборони держави автором розроблено єдиний підхід у Міністерстві оборони України, Збройних Силах України та Державній спеціальній службі транспорту України щодо реалізації заходів із підготовки та ведення кібероборони. На сучасному рівні, спираючись на досвід країн-партнерів НАТО обґрунтовано теоретичні засади нормативно-правового забезпечення діяльності у сфері кібероборони, в умовах набуття бойових спроможностей складниками сектору безпеки й оборони держави, запропоновано створення відповідних підрозділів виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту в зазначених вище структурах [1]. Визначено основні завдання системи кібероборони України.

Щоб визначити, яка модель системи кібероборони має стати для України нормативно врегульованою потрібно виконати дуже великий обсяг роботи. У даній статті автор спробує розібратися лише у концептуальному аспекті даної проблеми.

Отже, Україна взяла на себе зобов'язання перед НАТО та державами-партнерами щодо упровадження сучасних підходів до кібероборони, розвитку необхідних спроможностей сектору безпеки і оборони держави для дій у кіберпросторі та досягнення оперативної сумісності з питань забезпечення кібербезпеки з Альянсом [2]. Саме ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України" визначає, що на Міністерство оборони України (далі – Міноборони), Генеральний штаб Збройних Сил України покладені, відповідно до компетенції, завдання щодо здійснення заходів із підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони), здійснення військової співпраці з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз та упровадження заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану [3]. Тому відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захист технологічної інформації відповідно до вимог законодавства і буде покладена на зазначених вище суб'єктів забезпечення кібербезпеки.

Постановка проблеми в загальному вигляді. Безпекове середовище навколо України вимагає створення та функціонування комплексного єдиного підходу щодо системи кібероборони, який має включати визначення мети, цілей, принципів, напрямів, основних завдань, процедур створення та функціонування необхідних організаційних структур, підготовки та ведення дій у кіберпросторі [4], а також відповідних питань організації діяльності органів військового управління всіх рівнів, військ (сил), взаємодії та забезпечення відповідно до завдань, що виконують Міноборони, Збройні Сили України та Державна спеціальна служба транспорту України (далі – Держспецтрансслужба).

Отже, **мета статті** полягає в створенні та функціонуванні системи кібероборони України за умов реалізації заходів із підготовки та її ведення, враховуючи розроблення основних складників функціонування системи кібероборони, перспективи та напрями її використання в контексті реформування системи державного управління в Україні, враховуючи досвід формування засад у цій сфері публічного управління країнами-членами НАТО.

Виклад основного матеріалу. За останні 5–10 років численні наукові видання та інші публікації було присвячено перспективам реформування в Україні діючої моделі системи кібероборони, в тому чи іншому її прояві. Як взірець, матрицею реформ обиралася найпоширеніша у світі система кібероборони США, яка набула у країн-членів НАТО діючого статусу.

Такі ж самі устремління були характерні й для деяких пострадянських країн, країн Центральної та Східної Європи. Проте досвід останніх років для України свідчить про передчасність вказаних сподівань.

На думку українських експертів, обізнаних у суті проблеми, намагання більшості представників сектору безпеки держави відразу перестрибнути у сучасну систему управління без попереднього формування міцного підґрунтя у вигляді базових механізмів функціонування системи з чітким визначенням її призначення та характеристики були марними.

Автором акцентується увага саме на механізмах створення та функціонування системи кібероборони України за сучасних умов. Тому у цілому для створення та функціонування системи кібероборони держави характерними будуть такі складові, а саме:

1. Завчасне та всебічне нормативно-правове регулювання діяльності з кібероборони, розроблення концепцій, доктрин, програм.

Основні завдання:

– визначення переліку положень у сфері кібероборони, які потребують нормативно-правового врегулювання;

– проведення наукових досліджень щодо розроблення та обґрунтування теоретичних засад нормативно-правового забезпечення діяльності у сфері кібероборони;

– створення та розвиток вітчизняної термінологічної бази у сфері кібероборони;

– організація розроблення та імплементація концепцій, доктрин, програм, планів із питань підготовки та ведення кібероборони;

– відображення питань, що стосуються протидії кіберзагрозам у воєнній сфері, відбиття воєнної агресії в кіберпросторі, підготовки, ведення та забезпечення кібероборони, керівництва кіберобороною та її складниками в нормативно-правових актах держави з питань національної безпеки, відомчих нормативних документах [5];

– розроблення, періодичний перегляд, уточнення та переопрацювання відомчих керівних, планувальних та розпорядчих документів із питань кібероборони;

– розроблення та імплементація індикаторів та порядку оцінювання діяльності суб'єктів кібероборони та стану об'єктів кібероборони;

– розроблення та реалізація процедур інтеграції, взаємної сумісності з нормативними документами НАТО з питань кібербезпеки та дій у кіберпросторі;

– розроблення та приведення національних і військових стандартів за напрямом кібероборони у відповідність до міжнародних норм та стандартів, що застосовуються в Європейському Союзі (ЄС) та НАТО.

Очікуваний результат – створення нормативно-правової бази за напрямом підготовки та ведення кібероборони, організація здійснення постійного аналізу та своєчасного вдосконалення чинних нормативних документів за визначеним напрямом діяльності.

2. Випереджувальний розвиток організаційних структур в інтересах виконання завдань кібероборони.

Основні завдання:

– розвиток Збройних Сил для виконання завдань кібероборони шляхом створення нових (реорганізації тих, що існують) органів військового управління, військових частин (підрозділів у складі їх);

– створення (визначення) у складі Міноборони та Генерального штабу Збройних Сил, Держспецтрансслужбі підрозділів, відповідальних за організацію та планування заходів забезпечення кібербезпеки, включаючи кібероборону;

– розвиток спроможностей розвідувального органу Міноборони щодо дій у кіберпросторі;

– розвиток центрів (підрозділів) захисту інформації та кібербезпеки в інформаційно-телекомунікаційній системі Збройних Сил як основної платформи забезпечення комплексного кіберзахисту у воєнній сфері;

– розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил;

– створення та функціонування принципово нових інноваційних організаційних одиниць у складі органів управління та військ (сил) за напрямом

кібербезпеки, у т. ч. експериментальних, навчально-бойових, випробувальних тощо;

– створення підрозділів активного кіберзахисту, у т. ч. для виконання завдань пошуку вразливостей (тестування) власних інформаційно-телекомунікаційних систем, об'єктів інформаційної інфраструктури, імітації дій противника в кіберпросторі під час заходів підготовки військ (сил) тощо [6];

– створення підрозділів (мобільних груп реагування) для забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури держави;

– розвиток спроможностей щодо виконання завдань у кіберпросторі підрозділів, відповідальних за протидію технічним розвідкам;

– організаційне виокремлення та інтеграція сил та засобів Збройних Сил, основною сферою застосування яких є інформаційний (кібер) простір в окремий рід військ шляхом формування інтегрувального роду військ інформаційної підтримки (забезпечення) (як варіант – Командування інформаційного та кіберпростору Збройних Сил України), а також необхідних структур зазначеного спрямування в системі військової освіти та науки;

– розвиток спроможностей Сил спеціальних операцій Збройних Сил України для проведення спеціальних та інформаційно-психологічних операцій в інтересах кібероборони, у кіберпросторі та з використанням кіберпростору;

– розвиток організаційних та інших спроможностей Військової служби правопорядку у Збройних Силах України (після реформування – військової поліції) щодо проведення правоохоронних заходів в інтересах підготовки, ведення та забезпечення кібероборони;

– збереження та розвиток підрозділів військових навчальних закладів та науково-дослідних установ Збройних Сил, які здійснюють підготовку фахівців та наукові дослідження в інтересах кібероборони та інших заходів забезпечення кібербезпеки держави;

– сприяння розвитку спроможностей суб'єктів забезпечення кібербезпеки держави щодо участі їх у виконанні завдань кібероборони;

– розвиток мобілізаційної компоненти кібероборони шляхом використання складників (можливостей) мобілізації, військової служби в резерві, оперативного резерву, визначення мобілізаційних завдань тощо.

Очікуваний результат – створення відповідних організаційних структур, на які буде покладено завдання щодо організації та виконання заходів із кібероборони, набуття створеними підрозділами необхідних для успішного виконання завдань з кібероборони спроможностей.

3. Всебічна підготовка органів військового управління, військ (сил) до виконання завдань кібероборони.

Основні завдання:

– розроблення та упровадження системи підготовки органів військового управління, військ (сил) до виконання завдань кібероборони;

– опанування сучасних форм та способів виконання завдань щодо кібероборони (дій у кіберпросторі) загальновійськовими (видовими, міжвидовими тощо) органами військового управління всіх рівнів, військами (силами), родами військ;

– удосконалення системи охорони державної таємниці та іншої інформації з обмеженим доступом, захисту державних інформаційних ресурсів, технічного і криптографічного захисту інформації;

– участь визначених органів військового управління та підрозділів Міністерства оборони України, Збройних Сил України у проведенні навчань (тренувань) щодо захисту критичної інформаційної інфраструктури держави (у межах компетенції);

– участь органів військового управління та підрозділів Збройних Сил України у міжнародних навчаннях з кібероборони та забезпечення кібербезпеки.

Очікуваний результат – розроблення та упровадження комплексу заходів підготовки за напрямом "кібероборона" в рамках наявної системи підготовки органів військового управління, військ (сил).

4. Створення та розвиток матеріально-технічної основи кібероборони.

Основні завдання:

– створення та розвиток інформаційної інфраструктури системи Міноборони в інтересах підготовки та проведення кібероборони;

– створення (залучення) необхідної інформаційної інфраструктури держави всіх форм власності для її використання в інтересах кібероборони та періодичне проведення її огляду;

– забезпечення взаємосумісності інформаційно-телекомунікаційних систем, програмно-технічних засобів систем управління військами та зброєю Збройних Сил з аналогічними системами інших суб'єктів оборони та забезпечення кібербезпеки держави;

– проведення науково-дослідних та дослідно-конструкторських робіт щодо створення сучасних зразків зброї, програмно-технічних та інших засобів в інтересах виконання завдань кібероборони, забезпечення ними відповідних підрозділів у необхідній кількості;

– створення Єдиної автоматизованої системи управління Збройних Сил з урахуванням забезпечення її кібербезпеки на необхідному рівні;

– залучення можливостей структур громадянського суспільства (громадських організацій) до виконання завдань у сфері забезпечення кібероборони (на добровільних засадах);

– розширення співробітництва між державним і приватним секторами, залучення інноваційного потенціалу приватних компаній до наукових досліджень і розроблення рішень у сфері забезпечення кібероборони.

Очікуваний результат – створення в системі Міноборони інформаційної інфраструктури, сумісної з іншими складниками сектору оборони і безпеки, організація роботи щодо розроблення та упровадження нових зразків озброєння в інтересах підготовки та ведення кібероборони.

5. Формування й розвиток людського капіталу як головного чинника успішного виконання завдань кібероборони.

Основні завдання:

– створення привабливих умов для проходження військової служби в органах військового управління та підрозділах, на які покладаються виконання завдань кібероборони;

– пошук та залучення до військової служби у відповідних підрозділах обдарованої (талановитої) молоді;

– упровадження сучасних підходів до управління військовою кар'єрою на рівні підходів (стандартів, найкращих практик) збройних сил країн – членів НАТО, у т. ч. механізмів нестандартних індивідуальних підходів до найбільш цінних фахівців;

– створення та розвиток дієвої системи безперервної підготовки (навчання) та професійного вдосконалення протягом усієї кар'єри для фахівців із питань кібероборони, відповідного кадрового менеджменту в цій галузі та необхідного науково-виробничого потенціалу;

– запровадження механізмів персональної мотивації особового складу, який займає ключові посади в підрозділах, має унікальні професійні якості та здійснює значний персональний внесок в успішне виконання завдань за призначенням;

– надання можливостей щодо розвитку фахівців, у т. ч. шляхом навчання на базі цивільних навчальних закладів, стажування на базі провідних вітчизняних та зарубіжних ІТ-компаній, участі в конференціях, семінарах, інших заходах професійного розвитку.

Очікуваний результат – підрозділи, на які покладено завдання із кібероборони, повинно укомплектувати професійним та вмотивованим особовим складом, що, у свою чергу, сприятиме формуванню та упровадженню в Міноборони системи підвищення професійного рівня особового складу.

6. Набуття спроможностей та здійснення ефективного керівництва кіберобороною.

Основні завдання:

– зміна парадигми мислення та дій керівників (командирів) у бік набуття ними ментальної готовності та спроможностей виконання завдань (дій) у кіберпросторі та через кіберпростір;

– визначення (встановлення) цілей, що їх планується досягти в кіберпросторі в інтересах досягнення мети оборони держави (застосування Збройних Сил);

– визначення порядку керівництва підготовкою та веденням кібероборони;

– інтеграція заходів щодо підготовки та ведення кібероборони в діяльність органів військового управління всіх рівнів як невід'ємної частини керівництва підготовкою та застосуванням військ (сил) Збройних Сил;

– визначення переліку завдань з кібероборони, способів виконання їх та необхідних ресурсів;

– завчасне визначення об'єктів дій у кіберпросторі (ведення кібероборони), шляхів та способів отримання доступу до них та можливостей здійснення впливу;

– завчасне визначення порядку, встановлення та підтримання взаємодії з суб'єктами кібероборони;

- упровадження механізмів та процедур спільного застосування Збройних Сил та інших суб'єктів забезпечення кібербезпеки держави в інтересах ефективного виконання завдань кібероборони.

Очікуваний результат – створення системи управління системою кібероборони.

7. Ефективне виконання поточних заходів щодо випереджувального реагування на дії противника в кіберпросторі, підготовки та ведення Збройними Силами кібероборони.

Основні завдання:

– моніторинг кіберпростору, завчасне виявлення загроз;

– здійснення розвідувальним органом Міноборони розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки, вжиття заходів протидії зовнішнім загрозам національній безпеці України, у т. ч. у кіберпросторі [7];

– проведення інформаційно-аналітичної діяльності та прогнозування розвитку обстановки у воєнній сфері, пов'язаній із кіберзагрозами та кіберпростором;

– підтримання сил та засобів для дій у кіберпросторі в готовності до виконання завдань за призначенням, адекватне нарощування їхньої готовності залежно від рівня загроз та ступенів реагування на них;

– несення бойового чергування визначених сил та засобів в інтересах підготовки та ведення кібероборони;

– проведення поточних заходів підготовки та ведення кібероборони відповідно до компетенції (завдань) органів військового управління всіх рівнів, військових частин, організацій та установ Міноборони, Збройних Сил та Держспецтрансслужби;

– проведення оперативно-розшукових та інших правоохоронних заходів в інтересах кібероборони;

– випереджувальна перевірка на уразливість від кібервпливу об'єктів кібероборони, об'єктів критичної інформаційної інфраструктури;

– випереджувальне та/або оперативне реагування на проведення противником заходів у кіберпросторі та через кіберпростір, мінімізація результатів їхнього впливу. За необхідності – безпосереднє здійснення заходів кібервпливу та інших заходів у кіберпросторі та через кіберпростір, координація проведення та уточнення їх за необхідності;

– розвиток технологій кіберзахисту засобів рухомого зв'язку, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

– участь у забезпеченні кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка перебуває під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України [8];

– всебічна підготовка до проведення заходів кібероборони;

– створення, упровадження в суб'єктів кібероборони інформаційно-технологічних систем, програмно-апаратних комплексів, засобів кіберзахисту, кібервпливу, підготовка відповідних фахівців, формування та розиток відповідних підрозділів;

– упровадження дієвої системи захисту інформації та безпеки інформаційних ресурсів в системі Міноборони від кібервпливу (кібератак);

– здійснення поточних заходів військової співпраці з ЄС і НАТО, пов'язаної з безпекою кіберпростору та спільним захистом від кіберзагроз воєнного характеру;

– розвиток міжнародного співробітництва у сфері забезпечення кібероборони, підтримка міжнародних ініціатив, що відповідають національним інтересам України, поглиблення співпраці України з ЄС і НАТО для посилення спроможностей України у сфері забезпечення кібероборони, забезпечення участі в заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ;

– використання потенціалу державно-приватного партнерства, громадських організацій для виконання завдань у сфері забезпечення кібероборони.

Очікуваний результат – створення сприятливих умов у кіберпросторі, які забезпечать ефективну підготовку та застосування Збройних Сил щодо виконання завдань за призначенням.

Висновки з цього дослідження і перспективи подальших розвідок у цьому напрямі. Враховуючи новизну поняття "кібероборона", а також через відсутність єдиного підходу в Міноборони, Збройних Силах та Держспецтрансслужбі України щодо реалізації заходів із підготовки та ведення кібероборони, створення та функціонування системи кібероборони доцільно розглядати за деталізованими напрямами та завданнями, а саме:

1. Завчасне та всебічне нормативно-правове регулювання діяльності з кібероборони, розроблення концепцій, доктрин, програм.

2. Випереджувальний розвиток організаційних структур в інтересах виконання завдань кібероборони.

3. Всебічна підготовка органів військового управління, військ (сил) до виконання завдань кібероборони.

4. Створення та розвиток матеріально-технічної основи кібероборони.

5. Формування й розвиток людського капіталу як головного чинника успішного виконання завдань кібероборони.

6. Набуття спроможностей та здійснення ефективного керівництва кібероборoною.

7. Ефективне виконання поточних заходів щодо випереджувального реагування на дії противника в кіберпросторі, підготовки та ведення Збройними Силами кібероборони.

У подальшому функціонування системи кібероборони держави, щодо виконання завдань за призначенням безпосередньо залежатиме:

– від основних напрямів діяльності Міноборони, Збройних Сил та Держспецтрансслужби;

– набуття та подальшого розвитку необхідних і достатніх спроможностей Міноборони, Збройних Сил, Держспецтрансслужби для ефективних дій в інформаційному (кібер) просторі та досягнення оперативної сумісності з НАТО;

– практичного виконання поточних заходів щодо реагування на дії противника в кіберпросторі, підготовки та ведення Збройними Силами та Держспецтрансслужбою кібероборони в повсякденній діяльності, під час підготовки та застосування, у тому числі участі їх у проведенні операції Об'єднаних сил, антитерористичній операції.

Список використаних джерел

1. Орлов О. В., Онищенко Ю. М. Боротьба з кіберзлочинністю, як складова частина інформаційної безпеки країни в умовах глобалізації. *Сучасні проблеми правового, економічного та соціального розвитку держави* : тези доп. Міжнар. наук.-практ. конф. (м. Харків, 22 листоп. 2013 р.) ; МВС України, Харк. нац. ун-т внутр. справ. Харків, 2013. С. 418–420.

2. Матриця досягнення стратегічних цілей і виконання основних завдань оборонної реформи : Указ Президента України від 6 черв 2016 р. № 240. *Офіц. вісн. Президента України.* 2016. № 17. Ст. 466 (дата звернення : 13.05.2019).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2469-VIII. *ВВР України.* 2017. № 45. Ст. 403 (дата звернення : 10.05.2019).

4. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV. *ВВР України.* 2006. № 5. Ст. 128–71 (дата звернення : 11.04.2019).

5. Стратегія кібербезпеки України : Указ Президента України від 15 берез. 2016 р. № 96. *Офіц. вісн. Президента України*. 2016. № 10. Ст. 198.

6. Орлов О. В., Онищенко Ю. М. Протидія кіберзлочинності в умовах глобалізації суспільства. *Новітні інформаційно-комунікаційні технології в модернізації публічного*

управління: зарубіжний і вітчизняний досвід : матеріали наук.-практ. семінару, 19 квітня 2013 р., м. Дніпропетровськ. Дніпропетр. : ДРІДУ НАДУ, 2013. С. 74–77.

7. Кобзев І. В., Петров К. Е. Протидія злочинності як складова національної безпеки держави. *Актуальні проблеми розслідування кіберзлочинів : матеріали Всеукр. наук.-практ. конференції. м. Харків, 10 грудня 2013 р.* ; МВС України, Харк. нац. ун-т внутр. справ. Харків : ХНУВС, 2013. С. 101–103.

8. Orlov O. V., Kobzev I. V., Petrov K. E. Models and Foreign Experience of E-Goverment. *Problems of Developments Modern Science: Theory and Practice EDEX*, Madrid, Espana, 2016, P. 256–261.

References

1. Orlov, O.V., Onyschenko, Yu.M. (2013). Borotba z kiberzlochynnistiu, iak skladova chastyna informatsijnoi bezpeky krainy v umovakh hlobalizatsii. *Suchasni problemy pravovoho, ekonomichnoho ta sotsialnoho rozvytku derzhavy* : tezy dop. Mizhnar. nauk.-prakt. konf, 22 lystop. 2013 r. Kharkiv: nats. un-n-t vnutr. sprav, *418–420* [in Ukrainian].

2. Matrytsia dosiahnennia stratehichnykh tsilej i vykonannia osnovnykh zavdan oboronnoi reformy: Ukaz Prezydenta Ukrainy vid 06.06.2016 r. 240. (2016). *Ofitsijnyj visnyk Prezydenta Ukrainy, 17, art. 466* [in Ukrainian].

3. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. No 469-VIII. (2018). *Vidomosti Verkhovnoi Rady Ukrainy, 45, art. 403* [in Ukrainian].

4. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist': Zakon Ukrainy vid 07.09.2005 r. No 2824-IV. (2005). *Vidomosti Verkhovnoi Rady Ukrainy, 5, art. 128, art. 71* [in Ukrainian].

5. Stratehiia kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 15.03.2016 r. 96. (2016). *Ofitsijnyj visnyk Prezydenta Ukrainy, 10, 39, 198.Надійшла до редколегії 15.05.2019 р.*

6. Orlov, O.V., Onyschenko, Yu.M. (2013). Protydiia kiberzlochynnosti v umovakh hlobalizatsii suspil'stva. *Novitni informatsijno-komunikatsijni tekhnolohii v modernizatsii publichnoho upravlinnia: zarubizhnyj i vitchyznianyj dosvid* : materialy nauk.-prakt. seminaru, 19 kvit. 2013 r. Dnipropetrovs'k: Vyd-vo DRIDU NADU, *74–77* [in Ukrainian].

7. Kobzev, I.V., Petrov, K.E. (2013) Protydiia zlochynnosti iak skladova natsionalnoi bezpeky derzhavy. *Aktualni problemy rozsliduvannia kiberzlochyniv.* Materialy Vseukr. Nauk.-prakt. Konferentsii, 10 hrudnia 2013 r. Kharkiv: Vyd-vo KhNUVS, *101–103* [in Ukrainian].

8. Orlov, O.V., Kobzev, I.V., Petrov, K.E. (2016). Models and Foreign Experience of E-Government. *Problems of Developments Modern Science*. Theory and Practice EDEX, Madrid, *256-261* [in Espana].

Zhivilo Ye. O., *Postgraduate Student of Information Technologies and Control Systems Department, KRI NAPA, Kharkiv*
ORCID 0000-0003-4077-7853

THE ESSENCE OF THE MAIN TASKS OF THE UKRAINIAN CYBER DEFENSE SYSTEM

The article analyzes the essence of modern directions of creation and functioning of the cyber defense system of the state. It is determined that for modern Ukraine successful transition to the implementation of cyber defense training and maintenance measures is possible only if the directions and tasks of the cyber defense system are determined in advance.

The conclusions on the role of the existing political and legal course of functioning of the cyber defense system are formulated, further requirements for the acquisition of capabilities of the security and defense sector of the state in the cyber defense systems of Ukraine are formulated based on the best practices of the EU member states and NATO member states.

Keywords: cyber defense of the state, capabilities of the security and defense sector of the state, cyberspace, cyber threats, cyber defense of critical information infrastructure.

Надійшла до редколегії 15.05.2019 р.