УДК 94: [001+62](100)

Гула Р. В., Вітринська О. В.

КІБЕР-ЦАХАЛ[1] ПРОТИ КІБЕР-ДЖИХАДУ

В роботі зроблена спроба розкриття ретроспектив, зародження, розвитку та функціонування спецпідрозділів кіберзахисту держави Ізраїль під час протистояння з комплексом інформаційних загроз з боку країн-ворогів та організацій екстремістко-терористичного спрямування. Досліджені ознаки арабо-ізраїльського протистояння у сфері кібератак та кіберзахисту. Проаналізовані особливості підготовки спеціалістів воєнної ІТ сфери Ізраїлю. Проаналізовані характерні особливості кіберджихаду, та переваги його проведення, що надає мережа Інтернет. Вказано на роль релігійного чиннику у використанні людських ресурсів в організації кібератак і кібер-агресій в локальному сегменті та спрямування хакерської діяльності на комплекс об'єктів державної та приватної власності держави Ізраїль та її інформаційно-комунікаційну систему.

У XXI ст. людство остаточно перейшло в нову епоху, яка характеризується зростанням обсягу інформації, телекомунікаційним розвитком, удосконаленням інформаційних технологій, вільним доступом до інформаційних ресурсів, глобалізацією, модернізацією та інформатизацією усього суспільства.

Розвиток цивілізаційних процесів сучасності відбувається в умовах принципово нової філософсько-політологічної парадигми епохи постмодерну. Сучасними об'єктами наукового дискурсу є соціальні феномени коду та матриці. Кардинально переорієнтовується інформаційне протиборство, його завданнями стають переформатування ментальності нації та деформація патернів національної пам'яті, що зумовлено метою інформаційної війни.

На тлі цих світоглядних трансформацій уже шість десятиріч Близький Схід залишається найбільш напруженою зоною зіткнення цілого комплексу протиріч політичного, економічного, соціального, релігійного та навіть ментального протистояння Ізраїлю та арабського світу. Ескалація цих форм конфлікту в XX ст. уже декілька разів переростала в кровавi війни держави єврейського народу з арабськими країнами. Але на сучасному етапі історичної траєкторії розвитку глобалізаційних і модернізаційних змін сформувався унікальний феномен «віртуальної інформаційної політики», як реалізації та захисту національних інтересів у кіберпросторі, що в умовах стрімкого поширення новітніх інформаційних технологій вимагає побудови принципово нової ефективної інформаційної політики. Тому існує нагальна проблема дослідження та аналізу історичної ретроспективи трансформаційних процесів у створенні принципово нової моделі інформаційно-психологічного та інформаційно-технічного протистояння в кіберпросторі за умов ферментного загострення конфлікту між державою Ізраїль та арабським світом.

Наукові праці фахівців у галузі філософії, політології, загальної теорії держави та права, теорії управління, інформаційного права та безпекознавства В. П. Горбуліна, О. Г. Данільяна, О. С. Ліпкана, Ю. Є. Максименка, В. Л. Манілова, О. В. Манойла, Н. Р. Нижник, Д. М. Овсяника, В. В. Остроухова, І. Н. Панаріна, В. М. Петрика, Г. Г. Почепцова, В. Ф. Прокоф'єва, Г. П. Ситника, О. Ф. Скакун, Ю. М. Старилова, В. А. Тихонова, Л. С. Харченка, А. О. Фісуна, Д. Б. Фролова, Ю. С. Шемчученка, В. С. Цимбалюка, О. К. Юдіна та ін. стали науковим підґрунтям для поглибленого вивчення проблем розкриття змісту та сутності інформаційного протиборства та кібервійн. Варто також виокремити низку спеціальних монографічних праць російських, європейський та американських авторів з проблематики інформаційних війн, пропаганди та спеціальних інформаційних операцій С. Зуєва, Г. Ємельянова, А. Левакова, С. Расторгуєва, Дж. Арквіллі, Д. Кюля, Р. Моландера, Дж. Ная та інших.

[1] ЦАХАЛ – Армія Оборони Ізраїлю.

Ці автори започаткували та докладно розглянули загальне питання кібервійн та інформаційного протиборства. Проблема воєнного протистояння із застосуванням нових інформаційних технологій Ізраїлю та арабських країн в кіберпросторі побіжно згадується у їхніх дослідженнях. Значні складності для дослідників виникають у зв'язку з обмеженим доступом до інформації, яка містить державну та воєнну таємницю.

Автори роботи, користуючись комплексом інформації з відкритих джерел ставлять за мету розкриття ретроспективи, зародження, розвитку та функціонування спецпідрозділів кіберзахисту держави Ізраїль під час протистояння з комплексом інформаційних загроз з боку країн-ворогів та організацій екстремістко-терористичного спрямування.

Війну в кіберпросторі (кібервійну) в сучасному науковому дискурсі розглядають як форму розвитку та поширення інформаційних технологій у воєнній сфері, складову частину інформаційних війн, що здійснюється із використанням всесвітньої мережі [1, с. 20-23], і як «інформаційну війну, яку ведуть у кіберпросторі шляхом здійснення кібератак і захисту власної інфосфери» [2, с. 80].

Можна стверджувати, що, характерною рисою сучасного етапу інформаційного протистояння є відкриті зіткнення у кіберпросторі та збільшення впливу в інформаційній війні так званого медійного компоненту. Ресурсною базою цього виду «бойових дій» є рекрутовані спеціалісти IT технологій, хакери, активні «мешканці» блогосфери, які працюють у тісній взаємодії з державними ідеологічно-пропагандистськими структурами.

Головною особливістю сьогодення є те, що, завдяки цифровим технологіям, мережеві структури набувають характеру гнучких, адаптивних, децентралізованих елементів координованої системи. Ця система, незважаючи на автономність складників здатна до цілеспрямованих активних дій у відповідності з ухваленими рішеннями. Сучасне мережеве суспільство – це об'єктивна реальність, яка характеризується гіперсоціальністю. Але гіперсоціальність – це, за термінологією М. Кастельса, «мережевий індивідуалізм». Тобто це система, коли індивід сам обирає мережеву структуру за аксіологією власних уподобань. У сьогоднішньому глобалізованому світі мережеві структури протистоять суверенній державі з двох сторін – «знизу» у формі різних формальних і неформальних спільнот і недержавних організацій, та «верху», у вигляді «наддержавних мережевих структур [3, с. 43].

Не є виключенням у розвитку цих процесів і політика кіберзахисту власних національних інтересів і координації зусиль державних і недержавних інституцій у проведені акцій інформаційної агресії як зі сторони держави Ізраїль, так і з боку держав арабського світу й екстремістських угрупувань терористичній спрямованості.

Крайній ступень ідеологічного антагонізму та загострення протистояння в кіберпросторі між арабами та євреями викликав навіть появу терміну «кіберджихад». Уперше цей термін з'явився на початку 2000-х рр., у ході палестино-ізраїльського протистояння, коли Ізраїль був змушений відбивати одну за одною атаки палестинських хакерів на сайти державних і комерційних організацій [4]. Під терміном «кіберджихад» тоді розуміли несанкціоноване проникнення ісламістських хакерів в електронні системи «противника» зі зловмисної метою завдати цим системам збиток і порушити керованість органів військово-політичного управління.

Зараз можна стверджувати, що «кіберджихад» є формою кібертероризму (особливого різновиду психологічного терору, синтезованої форми інформаційно-психологічного насильницького впливу на суспільну свідомість та злочинного використання інформаційно-комунікативних систем, мереж та їх компонентів у кіберпросторі).

Тому вплив Інтернету в середовищі джихадистів обумовлено наступними чинниками:

– веб-сайти виступають у ролі віртуальних мечетей;

– віртуальні мережеві групи виникають у всьому світі в хаотичному порядку та можуть діяти ізольовано;

– Інтернет-технології залучають до віртуальних ісламістських мереж молодь і тих, хто цікавиться веб-програмуванням;

– Інтернет не накладає гендерних обмежень: жінки, які раніше були невидимою інфраструктурою джихаду, тепер можуть повноцінно брати участь у віртуальних ісламістських групах.

Крім цього, Інтернет також виконує інструментальну функцію, що дозволяє кібер-джихадістам:

– використовувати можливість анонімного розміщення інформації та отримання інструкцій;

– формувати світовий віртуальний майданчик для розповсюджувачів цілей, стратегії, тактики, і в цілому ідеології, та залученні споживачів цієї ідеології;

– забезпечити відносно безконфліктне співіснування численних конкуруючих джихадистських вебсайтів, що знижує внутрішню деградацію ісламістів;

– створити за допомогою віртуального командування нову модель «Джихаду без керівників», коли терористичну діяльність контролюють не «керівники», а учасники мережі [3, с. 45].

В Ізраїлі досвід здійснення вдалих інформаційних операцій під час ізраїльсько-арабських збройних конфліктів, дав можливість створити досить потужну систему інформаційно-пропагандистської роботи, функціонування якої забезпечують такі структури:

– відділ пропаганди при Міністерстві закордонних справ;

– відділ пропаганди при управлінні міжнародних відносин збройних сил країни;

– інформаційно-аналітичний відділ та відділ соціально-психологічних досліджень Головного штабу збройних сил Ізраїлю;

– управління військових рабинів збройних сил Ізраїлю;

– бюро пропаганди, яке координує дії єврейської діаспори;

– місцеві та закордонні засоби масової інформації;

– Інтернет ресурси [5, с. 30].

Ця система інформаційно-пропагандистської роботи дозволяє державним структурам Ізраїлю досить успішно вирішити цілий комплекс завдань, а саме:

– сформувати негативний імідж руху ХАМАС[1] як агресора та показати Ізраїль, як країну, яка вимушена давати адекватну відповідь агресору під час боротьби з тероризмом;

– досягнути суттєвого ослаблення ХАМАСу з боку країн-лідерів регіону та своїх ключових союзників;

– попередити і мінімізувати прогнозовану негативну реакцію в світі на наслідки можливих контртерористичних операцій ЦАХАЛу з неминучими жертвами серед мирного населення та зруйнуванням інфраструктури об'єктів ведення бойових дій.

В останнє десятиріччя досягнення цих результатів все частіше відбувається у площині комп'ютерних мереж. Наприклад, під час операції «Литий свинець» (ізраїльська військова операція в Секторі Газа (27.12. 2008 – 18.01.2009) метою якої ставилося знищення військової інфраструктури правлячого в Газі ісламського радикального руху ХАМАС) інтернет-ресурси ХАМАСу вивели з ладу низку ізраїльських фірм, які пов'язані із високими технологіями, телекомунікаціями, електронної комерцією, а також ЗМІ та медичні заклади. На деякий час були навіть заблоковані сайти міністерства оборони і зовнішніх справ.

У відповідь хакери Ізраїлю заблокували майже 50 сайтів руху «Хезболла», міністерства сільського господарства Ірану, торговельних компаній Йорданії та Лівану, які були пов'язані з діяльністю ХАМАСу. Відносно пропалестинських російсько-, англо-, арабомовних сайтів була спланована вдала кібератака ізраїльських хакерів.

Реальність і масштабність інформаційних загроз національній безпеці держав у сучасному глобальному інформаційно-комунікаційному середовищі зумовили створення спеціалізованих підрозділів у правоохоронних органах і збройних силах країн, так званих кібервійськ. На нашу думку, кібервійська (Сили кібероперацій – СкбО) – це спеціальні

[1] ХАМАС – палестинський ісламський рух опору, політична партія.

військові формування у складі збройних сил, які за своїм функціональним призначення забезпечують комплексний захист інформаційно-комунікаційної інфраструктури національної безпеки держави від несанкціонованого втручання зі сторони державних, недержавних і транснаціональних кіберугрупувань, доступ до комп'ютерних мереж імовірного супротивника та використання їх у власних інтересах через застосування новітніх ІТ технологій силами професійних комунікаторів та фахівців із ведення інформаційної війни [6, с. 219].

У 2012 р. були вперше відкрити курси з кіберзахисту для офіцерів ЦАХАЛу. Інтенсифікований навчальний процес включав 13-годинний навчальний день і два заліки щодня. З метою відпрацювання навичок фахівці створили для курсантів ізольовану комп'ютерну мережу. Вже на початок 2013 р. Армія Оборони Ізраїлю подвоїла кількість офіцерів у структурах, які на той час займалися питаннями кіберзахисту [7].

За інформацією з відкритих джерел у ЦАХАЛі з 2013 р. було проголошено про початок процесу створення спеціальних підрозділів кібератак і кіберзахисту. Ізраїльський веб-сайт «Курсорінфо» від 16 липня 2013 р. інформував своїх читачів, що начальник генерального штабу Армії Оборони Ізраїлю генерал-лейтенант Гаді Айзенткот наказав сформувати новий вид військ, який буде займатися веденням кібервійни і відбиттям кібератак противника. Паралельно голові військової розвідки Херцу Халеві було наказано визначити напрями дій кібервійськ в оборонній і в наступальній сфері. Новий рід військ планувалося сформувати поетапно впродовж двох років [8].

Організаційне будівництво нових структур кіберзахисту було розпочато після заяви прем'єр-міністра Ізраїлю Біньяміна Нетаніягу в червні 2013 р. про створення Національної цільової кібернетичної групи для захисту життєво важливих об'єктів інфраструктури Ізраїлю [9]. Вже у серпні 2013 р. армія взяла на службу близько 300 молодих комп'ютерних фахівців, причому багато хто з них не закінчив коледж або не мав повної шкільної освіти, але в той же час вони були визнаними фахівцями у сфері комп'ютерних технологій. Новобранці проходили службу в підрозділі військової розвідки 8200, а також в Управлінні командування, контролю, зв'язку, комп'ютерів і розвідки С4І. Власне на базі цих двох підрозділів було розпочато процес створення кібервійськ ЦАХАЛу. Ключовим завданням кібервійськ стало підвищення рівня оборони Ізраїлю та координація розробки нового програмного забезпечення між армією й ізраїльськими компаніями сектора високих технологій [10].

Але вже на початку 2017 р. начальник генерального штабу Армії Оборони Ізраїлю генерал-лейтенант Гаді Айзенкот прийняв рішення не створювати новий вид військ, який буде відповідати за кібербезпеку. На цей час відповідальність за управління та координації дій кіберзахисту збройних сил Ізраїлю покладена на Управління зв'язку та кіберзахисту Генерального штабу ЦАХАЛу, а за атакуючі дії на кіберфронті відповідає розвідувальне управління (АМАН) [11].

Тому побудова системи кіберзахисту Армії Оборони Ізраїлю відбувається на основі створення структурних підрозділів видів військ і включення елементів кіберзахисту армії до єдиної державної інформаційно-технічної інфраструктури.

У грудні 2017 р. був сформований окремий напрям кіберзахисту в складі Сухопутних військ. Новий підрозділ входив до організаційно-штатної структури відділу зв'язку штабу Сухопутних військ. Завданнями напряму кіберзахисту визначено забезпечення захисту всіх видів озброєння та військової техніки Сухопутних військ, що мають комп'ютерні системи, від взлому або захоплення контролю. Напрям кіберзахисту складається з 4 секторів, які відповідають за розробку засобів захисту, впровадження їх у бойову техніку та розробку планів розвитку. Кадрове забезпечення здійснене за допомогою фахівців Головного управління зв'язку Головного Штабу, в тому числі управління захисних систем, різних комп'ютерних підрозділів [12] та бази підготовки – школи комп'ютерних професій «БИС ля-Макциот ха-Махшев». Основною формою бойового навчання структур кіберзахисту ЦАХАЛу є навчання та тренування відбиття можливих інформійно-технічних атак зі сторони ворога [13].

За планами ізраїльського політичного керівництва структури кіберзахисту Армії Оборони Ізраїлю тісно взаємодіють із компонентами єдиної державної системи боротьби з кібертероризмом. 15 лютого 2015 р. на щотижневому засіданні уряду Ізраїлю було затверджено рішення про створення нового державного органу Управління по боротьбі з кібернетичної загрозою. Планувалося, що управління буде займається комплексним захистом від кібератак, у тому числі відпрацюванням загроз і атак в реальному часі. При управлінні також мав працювати національний центр підтримки CERT (Cyber Event Readiness Team) для боротьби з кіберзагрозами з метою забезпечення захисту різних організацій і галузей [14]. Завдання Управління – координувати відображення атак у кібернетичному просторі, які, за словами прем'єр-міністра Біньяміна Нетаніягу, «здатні паралізувати цілі країни». Формування державної інституції з істотно ширшими оперативними повноваженнями і завданнями значно підвищило статус органу координаційного центру протидії кібертероризму країн-супротивників [15]. Створення його структури відбувається поетапно, протягом трьох років. Нове керівництво працює спільно з нині чинним національним штабом з кібербезпеки. Управління та штаб утворюють єдину систему національної кіберзахисту при міністерстві глави уряду.

Окрім побудови організаційно-штатної структури ізраїльська влада приділяє велику увагу розвитку інформаційно-технічної інфраструктури для захисту національних інтересів. 15 серпня 2018 р. уряд Ізраїлю оголосив про початок трьохрічної програми розвитку технологій інформаційної безпеки, намагаючись зробити країну лідером у цьому напрямку. Інвестиції в проект складуть 90 млн. шекелів (близько $ 24 млн. за курсом на момент анонса) [16].

Отже, Армії Оборони Ізраїлю вдалося побудувати ефективну та збалансовану систему кіберзахисту на основі систематизованої концепції ізраїльського політичного керівництва. Відмовившись від затратного шляху формування окремого виду військ, підрозділи кіберзахисту ЦАХАЛу органічно вбудовані до загальнодержавної структури інформаційно-психологічного та інформаційно-технічного захисту, що дозволяє успішно виконувати завдання протидії інформаційного впливу супротивника в умовах перманентного загострення воєнно-політичної обстановки в регіоні.

У контексті дослідженої проблеми потребують подальшого вивчення наступні питання:

- аналіз ефекту інформаційно-пропагандистського впливу сучасної системи інформаційного захисту військ і населення;
- попередня оцінка результатів цієї дії цієї системи унаслідок прийняття нової законодавчої бази інформаційної та кібербезпеи Ізраїлю з метою врахування їхніх висновків для побудови стратегії кіберзахисту України;
- вивчення комплексу потенційних загроз національній безпеці Ізраїлю в інформаційному просторі з боку держав-супротивників, держав-конкурентів;
- з'ясування стану інформаційної оборони України та обґрунтування пропозицій щодо її вдосконалення.

1. Польских Л. О применении глобальной компъютерной сети Интернет в интересах информационного противоборства / Л. Польских // Зарубежное военное обозрение. – 2005. – № 7. – С. 20–23.

2. Климчук О. О. Кібервійна в сучасних умовах / О. О. Климчук, Р. М. Кравченко // Інформаційна безпека людини, суспільства, держави. – 2011. – № 1(5). – С. 78–84.

3. Сурма И. В. Виртуальные войны за реальное геополитическое пространство: этиология джихада и киберджихада // Rocznik bezpieczeństwa międzynarodowego 2016. – vol. 10. – № 2. – С. 41–50.

4. Борисов С. Израиль и электронный джихад / С. Борисов [Електронний ресурс]. Режим доступу: www.pravda.ru/world/02-08-2001/803616-0/. – Назва з екрану.

5. Певцов В. Информационное противостояние организации ХАМАС и Израиля в новом тысячелетии / В. Певцов // Зарубежное военное обозрение. – 2013. – № 6. – С. 28–33.

6. Інформаційна війна і національна безпека: монографія / [П.П. Ткачук, Р.В. Гула, О.І. Сивак та ін.]. – Львів: АСВ, 2015. – 263 с.

7. ЦАХАЛ усиливает киберзащиту [Електронний ресурс] // jewish.ru. 13.01. 2013. – Режим доступу: https://jewish.ru/ru/news/articles/158611/. – Назва з екрану.

8. Начальник генштаба ЦАХАЛа приказал начать формирование кибервойск [Електронний ресурс] // Cursorinfo. – Режим доступу: https://cursorinfo.co.il/. – Назва з екрану.
9. Йак И. Израиль успешно противостоит врагу в киберпространстве [Електронний ресурс] // 7 канал, 10.06.2013. – Режим доступу: https://www.7kanal.co.il/News/News.aspx/160803. – Назва з екрану.
10. ЦАХАЛ формирует новые кибер-войска [Електронний ресурс] // Mignews. – Режим доступу: http://mignews.com/news/130112_104545_00238.html. – Назва з екрану.
11. Начгенштаба ЦАХАЛа отказался от идеи создания войск кибербезопасности [Електронний ресурс] // NEWSRU.CO.IL. – Режим доступу: http://m.newsru.co.il/israel/02jan2017/cyber303.html. – Назва з екрану.
12. Направление Киберзащиты СВ АОИ [Електронний ресурс] // CYCLOWIKI.ORG. – Режим доступу: http://cyclowiki.org/wiki/%D0%9D%D. – Назва з екрану.
13. «צה"ל של התמרון את שיבשה לא סייבר תקיפת שום» [Електронний ресурс] // ISRAEL DEFENCE. – № 8, 2018. – Режим доступу: http://www.israeldefense.co.il/he/content. – Назва з екрану.
14. 2015: Национальное управление по киберзащите создадут в Израиле [Електронний ресурс] // TADVISER. – Режим доступу: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Израиль#2015:_ . – Назва з екрану
15. Правительство утвердило создание новых «кибервойск» [Електронний ресурс] // NEWS.RAMBLE. – Режим доступу: http://news.rambler.ru/27363679/. – Назва з екрану.
16. Запуск трехлетней программы развития технологий кибербезопасности [Електронний ресурс] // TADVISER. – Режим доступу: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Израиль#. – Назва з екрану.

В работе проанализированы особенности информационного противостояния в глобализированном мире в условиях принципиально новых трансформационных изменений в парадигме постмодерна. Указано на значительную роль виртуального общества, блогосферы, в формировании коллективной и индивидуальной идентификации индивида и группы. Выявлены и исследованы принципиально новые черты функционирования виртуального общества как новой формы социума в условиях процессов глобализации и модернизации общества.

Сделана попытка раскрытия ретроспективы, зарождения, развития и функционирования спецподразделений киберзащиты государства Израиль во время противостояния с комплексом информационных угроз со стороны стран-врагов и организаций экстремистско-террористического направления.

Выделены особенности арабо-израильского информационного противостояния в кибер-пространстве. Проанализирована структура органов власти Израиля, которые занимаются ведением информационной войны, и их задания в условиях трансформации взглядов военно-политического руководства на роль и место кибервойск в системе национальной обороны. Исследованы особенности подготовки специалистов военной IT сферы. Указанно на особенности применения информационно-психологической и информационно-технической составляющей в построении структуры киберзациты государства Израиль.

Создание новой модели киберзащиты государства Израиль было основано на координации деятельности государственных учреждений и политических институтов в организации системы киберзащиты; привлечении общественного сегмента в работе государственных структур с целью защиты национальных интересов в киберпространстве; использовании системного подхода к вопросам информационно-психологического и информационно-технического противостояния.

Исследованы признаки современного этапа противостояния в сфере кибератак и киберзащиты.

Проанализированы характерные особенности киберджихада и его преимущества, которые предоставляет сеть Интернет. Определена роль религиозного фактора в использовании человеческих ресурсов в организации кибератак и киберагрессии в локальном сегменте и направление хакерской деятельности на комплекс объектов государственной и частной собственности в государстве Израиль ее информационно-коммуникационную систему.

Authors have analyzed features of information opposition in the globalized world in the conditions of essentially new transformational changes in a postmodern paradigm. The significant role of virtual

society, a blogosphere of in formation of collective and individual identification of a person and a group are revealed. Essentially, new lines of functioning of virtual society as new forms of society in the conditions of processes of globalization and modernization of society are investigated.

The attempt of disclosure of a retrospective, origin, development and functioning of special forces of cyber defense of the State of Israel during opposition with a complex of information threats from the countries enemies and the organizations of the extremist and terrorist direction is made.

Features of the Arab-Israeli information opposition in a cyber-space are marked out. The structure of authorities of Israel which are engaged in conducting information war and their tasks in the conditions of transformation of views of the military-political management for a role and the place of cyber-troops in the system of national defense is analyzed. The specifics of training of specialists military IT spheres are analyzed. Features of application of an information and psychological and information and technical component in creation of structure of cyber-defense of the State of Israel are defined.

Creation of new model of cyber-defense of the State of Israel has been based on use of system approach to questions of information and psychological and information and technical opposition; coordination of activity of public institutions and political institutes in the organization of system of cyber-defense; attraction of a public segment in work of government institutions for the purpose of protection of national interests in a cyber-space. Signs of the present stage of opposition in the sphere of cyber-attacks and cyber defense are investigated.

Characteristics of cyber-jihad and its advantage which are provided for his carrying out by the Internet are analyzed. The role of a religious factor in use of human resources in the organization of cyber-attacks and cyber-aggression in local a segment and the direction of hacker activity on a complex of objects of the state and private property in the State of Israel her information and communication system is investigated.

Keywords: cyber-defense, cyber-attack, information confrontation, information war, social and communication technology, Jihad.

1. Polskikh L. O primenenii globalnoy kompyuternoy seti Internet v interesakh informatsionnogo protivoborstva / L. Polskikh // Zarubezhnoye voyennoye obozreniye. – 2005. – № 7. – S. 20–23.

2. Klymchuk O. O. Kiberviina v suchasnykh umovakh / O. O. Klymchuk, R. M. Kravchenko // Informatsiina bezpeka liudyny, suspilstva, derzhavy. – 2011. – № 1(5). – S. 78–84.

3. Surma I. V. Virtualnyye voyny za realnoye geopoliticheskoye prostranstvo: etiologiya dzhikhada i kiberdzhikhada // Rocznik bezpieczeństwa międzynarodowego 2016. – vol. 10. – № 2. – C. 41–50.

4. Borisov S. Izrail i elektronnyy dzhikhad / S. Borisov[Elektronniy resurs]. – Rezhim dostupu: www.pravda.ru/world/02-08-2001/803616-0/. – Nazva z ekranu.

5. Pevtsov V. Informatsionnoye protivostoyaniye organizatsii KhAMAS i Izrailya v novom tysyacheletii / V. Pevtsov // Zarubezhnoye voyennoye obozreniye. – 2013. – № 6. – S. 28–33.

6. Informatsiina viina i natsionalna bezpeka: monohrafiia / [P.P. Tkachuk, R.V. Hula, O.I. Syvak ta in.]. – Lviv: ASV, 2015. – 263 s.

7. TsAKhAL usilivayet kiberzashchitu [Elektronniy resurs] // jewish.ru. 13.01. 2013. – Rezhim dostupu: https://jewish.ru/ru/news/articles/158611/. – Nazva z ekranu.

8. Nachalnik genshtaba TsAKhALa prikazal nachat formirovaniye kibervoysk [Elektronniy resurs] // Cursorinfo. – Rezhim dostupu: https://cursorinfo.co.il/. – Nazva z ekranu.

9. Yak I. Izrail uspeshno protivostoit vragu v kiberprostranstve [Elektronniy resurs] // 7 kanal. 10.06.2013. – Rezhim dostupu: https://www.7kanal.co.il/News/News.aspx/160803. – Nazva z ekranu.

10. TsAKhAL formiruyet novyye kiber-voyska [Elektronniy resurs] // Mignews. – Rezhim dostupu: http://mignews.com/news/130112_104545_00238.html. – Nazva z ekranu.

11. Nachgenshtaba TsAKhALa otkazalsya ot idei sozdaniya voysk kiberbezopasnosti [Elektronniy resurs] // NEWSRU.CO.IL. – Rezhim dostupu: http://m.newsru.co.il/israel/02jan2017/cyber303.html. – Nazva z ekranu.

12. Napravleniye Kiberzashchity SV AOI [Elektronniy resurs] // CYCLOWIKI.ORG. – Rezhim dostupu: http://cyclowiki.org/wiki/%D0%9D%D. – Nazva z ekranu.

13. «צה"ל של התמרון את שיבשה לא סייבר תקיפת שום» [Elektronniy resurs] // ISRAEL DEFENCE. – № 8, 2018– Rezhim dostupu: http://www.israeldefense.co.il/he/content. – Nazva z ekranu.

14. 2015: Natsionalnoye upravleniye po kiberzashchite sozdadut v Izraile [Elektronniy resurs] // TADVISER. – Rezhim dostupu: http://www.tadviser.ru/index.php/Statia:Kiberprestupnost_i_kiberkonflikty_:_Izrail#2015:_ . – Nazva z ekranu.

15. Pravitelstvo utverdilo sozdaniye novykh «kibervoysk» [Elektronniy resurs] // NEWS.RAMBLE. – Rezhim dostupu: http://news.rambler.ru/27363679/. – Nazva z ekranu.

16. Zapusk trekhletney programmy razvitiya tekhnologiy kiberbezopasnosti [Elektronniy resurs] . – Rezhim dostupu: http://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Израиль# – Nazva z ekranu.

Стаття надійшла до редколегії 6.06.2018 р.