УДК 659.4:327.88

КОМАРОВА Лариса Олексіївна
ТКАЧЕНКО Олексій Петрович

НАПРЯМИ ТА ПЕРСПЕКТИВИ ВЗАЄМОДІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ З КРАЇНАМИ – ЧЛЕНАМИ ОРГАНІЗАЦІЇ ГУАМ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ КІБЕРЗАГРОЗАМ

Постановка проблеми. Аналіз кібератак на критичну інформаційну інфраструктуру держави, підвищення їхньої складності та розширення відповідного інструментарію свідчать про причетність недружніх країн, насамперед Російської Федерації, до посягань на український кіберпростір: фактично Україна стала полігоном для апробації нових зразків кіберзброї та відповідних комбінаторних стратегій.

Враховуючи транскордонність сучасних кіберзагроз та пріоритетність євроатлантичного курсу нашої держави, важливим вектором діяльності Служби безпеки України стало налагодження дієвої взаємодії з міжнародними партнерами з протидії кібертероризму та гібридній агресії у кіберпросторі.

Із цією метою СБ України встановлено та забезпечено підтримання високого рівня взаємодії зі спецслужбами та правоохоронними органами країн Європи, Азії та Північної Америки, а також ключовими міжнародними організаціями – ОБСЄ, Радою Європи, НАТО, ООН тощо.

Останнім часом позиція Служби безпеки України у вирішенні низки питань є проактивною, вона виступає ініціатором нововведень у сфері регіональної та міжнародної кібербезпеки у відповідних організаціях.

Аналіз останніх досліджень і публікацій. Проблематику організації Службою безпеки України міжнародного співробітництва у сфері кібербезпеки в межах міжнародних і регіональних організацій розглядали такі вітчизняні фахівці: С. Бондаренко, О. Климчук, Д. Мельник, В. Петров, С. Петров, Н. Ткачук, В. Хлевицький та інші [2].

Однак у їхніх наукових роботах не висвітлено особливості міжнародного співробітництва у сфері забезпечення кібербезпеки та протидії кіберзагрозам Служби безпеки України з відповідними спеціальними та правоохоронними органами країн – членів Організації за демократію та економічний розвиток ГУАМ.

Мета роботи – дослідити питання міжнародного співробітництва СБ України у сфері забезпечення кібербезпеки в межах діяльності

міжнародних і регіональних організацій, встановити основні чинники, які на сьогодні сприяють або ускладнюють ефективність указаного співробітництва, та запропонувати шляхи покращання такої міжнародної взаємодії.

Виклад основного матеріалу. Збройна агресія РФ проти України розпочалася у лютому 2014 року, коли, порушивши фундаментальні принципи і норми міжнародного права, низку двосторонніх і багатосторонніх угод, російська регулярна армія захопила Кримський півострів. Це стало лише першим кроком, спрямованим на підрив державності та суверенітету України.

Цілковита реалізація цих планів була зірвана, однак російські регулярні війська та підконтрольні їм збройні формування, які складалися з російських найманців і завербованих місцевих мешканців, окупували окремі райони Донецької та Луганської областей України.

Водночас із метою дестабілізації внутрішньополітичної ситуації в Україні та послаблення економічного потенціалу зазначені дії російської сторони супроводжувалися низкою кібернетичних атак на об'єкти критичної інформаційної інфраструктури.

Останнім часом постійно зростає кількість і складність таких атак на ключові об'єкти енергетики, транспортного та фінансового секторів, сфери військово-промислового комплексу, а також на інформаційні системи органів державної влади України. Подібні кібератаки використовуються як для здійснення акцій кібершпигунства, так і для виведення з ладу об'єктів критичної інфраструктури – кібертероризму. Це засвідчує низка прикладів, зокрема:

– у 2014 році під час виборів Президента України відбувся злам комп'ютерних систем ЦВК, що призвело до спотворення процесів обробки інформації про хід голосування, а хибна інформація, викладена на зламаній вебсторінці сайту виборчої комісії, використана для дискредитації виборів;

– наприкінці 2015 року шкідливим програмним забезпеченням BlackEnergy виведено з ладу комп'ютерні мережі енергетичних підприємств західних та центральних регіонів України, унаслідок цього залишилися без електропостачання сотні тисяч споживачів цих енергокомпаній і виникли передумови до зростання соціальної напруженості в державі;

– у грудні 2016 року здійснено комплекс потужних кібератак на фінансовий сектор і транспортні підприємства України, на деякий час було призупинено обслуговування клієнтів державними фінансовими установами й транспортними компаніями;

– у червні 2017 року відбулася потужна кібератака світового масштабу (відома як Petya) на комп'ютерні мережі банківського, енергетичного, транспортного секторів, об'єктів зв'язку й інших важливих об'єктів критичної інфраструктури, епіцентром якої стала Україна.

Відповіддю масштабному зростанню рівня загроз та їхньому новому формату став перегляд підходів України загалом і Служби безпеки України, як провідного державного органу у сфері забезпечення

кібербезпеки зокрема, до виконання своїх завдань з урахуванням вимог сьогодення.

Організаційну складову системи кібербезпеки в СБУ становить створений у 2021 році у складі Національної академії Служби безпеки України Центр кібербезпеки (далі – Центр КБ) Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій. Розвиток Центру КБ передбачається у плідній взаємодії з партнерськими спецслужбами, допомозі партнерів із країн Західної Європи, США та реалізації програм у межах Трастового Фонду Україна–НАТО з питань кібербезпеки. Центр КБ разом із підрозділом забезпечення кіберзахисту Держспецзв'язку України повинен стати першим системним центром професійної компетенції з підготовки кадрів та із забезпечення професійної сертифікації фахівців із кібербезпеки на державному рівні.

На базі Центру КБ мають формуватися сучасні наукові та криміналістичні лабораторії, у яких досліджуватимуться нові форми й методи проведення кібератак і протидії їм. Напрями тренінгових сценаріїв повинні бути спрямовані на моделі реалізації процедур атак та випробування програмно-апаратних засобів протидії кіберзагрозам. Зрозуміло, що необхідно впроваджувати інтегровані цикли навчань і тренінгів для постійного підвищення професійного рівня як фахівців центральної ланки управління СБУ, так і співробітників регіональних органів СБУ, що протидіють кібернетичній агресії на місцях. Постійне підвищення професійного рівня та вивчення сучасних напрацювань у напрямі кібербезпеки дасть змогу СБ України на високому професійному рівні взаємодіяти та спілкуватись зі світовими лідерами в цій галузі й діяти на упередження різних класів загроз.

Перед Центром КБ на сьогодні постає завдання не лише забезпечувати професійну підготовку кадрів СБУ, а також проводити науково-практичні дослідження з напрямів забезпечення інформаційної безпеки та кібербезпеки об'єктів критичної інфраструктури, інтегрувати результати аналізу великих обсягів інформації, прогнозувати можливі цілі для атак і методи їх реалізації та своєчасно протидіяти їм.

Аналіз інструментарію, який застосовується проти нашої країни в кіберпросторі, дав можливість керівництву країни розробити обґрунтовані запобіжні заходи для підвищення кібербезпеки. За ініціативою СБУ Указом Президента України використання окремих програмних продуктів російського походження, що слугували елементною базою кібернападів, заборонено через механізм застосування санкцій до комерційних структур держави-агресора.

Водночас новим елементом кіберзагроз для України є комбінаційне поєднання акцій кібершпигунства та інформаційних спеціальних операцій, що несуть загрозу не тільки в кіберпросторі, а й у площині суспільно-політичних відносин.

Одним із головних факторів забезпечення кібербезпеки країни є поглиблення державно-приватного партнерства, оскільки жодна країна у

світі не може самотужки гарантувати стовідсоткову безпеку своїх інформаційних систем.

СБУ вживає системних заходів щодо підвищення рівня державно-приватного партнерства, яке є невід'ємною умовою розбудови ефективної системи кібербезпеки як складової системи національної безпеки України у відповідності до стандартів ЄС і НАТО.

Створено умови для розширення участі громадянського суспільства (ІТ-фахівців і приватних суб'єктів сфери кібербезпеки) у заходах із протидії кіберзагрозам державній безпеці.

Створено механізм обміну інформацією в режимі реального часу про виявлені кіберінциденти та кібератаки стосовно об'єктів критичної інфраструктури (насамперед банківської сфери, транспортної галузі, сфери зв'язку та телекомунікацій, енергетики тощо).

Завдяки вжитим заходам СБУ зміцнюються партнерські відносини з бізнесом і громадянським суспільством, що ґрунтуються на довірі та спільному прагненні подолати загрози в кіберпросторі нашої держави.

Розширюється географія джерел, з яких фахівці СБУ отримують унікальні дані щодо нових підходів до забезпечення кібербезпеки, зростає обмін інформацією зі світовими центрами компетенції в питаннях кібербезпеки.

Необхідно зазначити, що, незважаючи на те, що агресія РФ у кіберпросторі завдала значних збитків нашій державі, вона стала поштовхом і прискорила розбудову національної системи кібербезпеки, прийняття базових нормативно-правових актів у цій сфері, створення відповідних інституцій, удосконалення міжвідомчої взаємодії та координації, а також поглиблення державно-приватного партнерства та міжнародної співпраці.

Враховуючи транскордонний характер сучасних кіберзагроз, Служба безпеки України налагодила ефективну взаємодію з партнерськими спеціальними службами та правоохоронними органами, міжнародними організаціями, що спеціалізуються на кібернетичній безпеці.

Так, зокрема, налагоджено оперативний інформаційний обмін щодо виявлених кібератак, механізмів їх реалізації та потенційних загроз кібербезпеці зі спецслужбами та правоохоронними органами США, Канади, Ізраїлю, Туреччини, Південної Кореї, Японії, Великої Британії, Франції, Німеччини, Голландії, Польщі, Естонії, Литви та інших країн.

Служба безпеки України постійно бере активну участь у засіданнях Організації за демократію та економічний розвиток ГУАМ (далі – ГУАМ).

Так, зокрема, у 2012 році в складі ГУАМ була створена робоча підгрупа по боротьбі з кіберзлочинністю, ініціатором цього виступила СБ України. Ця підгрупа була перейменована на Робочу групу з кібербезпеки (далі – РГК) у 2014 році.

У межах роботи РГК, засідання якої відбувається двічі на рік, вирішуються питання щодо вдосконалення спроможностей держав-членів у сфері протидії кіберзагрозам,

обміну досвідом та співробітництва в зазначеній сфері.

У 2016 році РГК було вирішено розробити Меморандум про співробітництво країн – членів ГУАМ у сфері кібербезпеки. Наразі обговорюються положення вказаного Меморандуму та можливість його ухвалення країнами – членами ГУАМ на національному рівні. Проєкт цього документа погоджений на національному рівні урядами Азербайджану та Грузії. В Україні проєкт Меморандуму пройшов процедуру міжвідомчого погодження.

Під час чергового засідання Робочої групи ГУАМ з кібербезпеки, яке відбулось у січні 2019 року, разом з іншими обговорювалося питання можливості та доцільності створення в Україні Регіонального центру ГУАМ у сфері кібербезпеки (далі – Центр).

Створення вказаного Центру було запропоновано українською стороною під час зустрічі країн – учасниць Організації за демократію та економічний розвиток ГУАМ на рівні голів урядів за участі Президента України, яка відбулась 27 березня 2017 року в м. Києві.

Враховуючи, що останнім часом Україна стала об'єктом кібератак, джерела яких походять із Російської Федерації, на думку СБ України, створення Регіонального центру ГУАМ у сфері кібербезпеки в Україні сприятиме зміцненню потенціалу у забезпеченні кібербезпеки країн – членів ГУАМ.

Крім того, вбачається, що функціонування вказаного центру на території нашої країни, ураховуючи наявні міжнародні контакти в межах НАТО, ЄС, Ради Європи, ОБСЄ, допоможе створити для країн – членів ГУАМ додаткові механізми обміну світовими практиками в галузі кібербезпеки та боротьби з кіберзлочинністю, дасть змогу підвищити рівень фахівців країн – членів ГУАМ у цих галузях та сприятиме покращанню іміджу цієї організації на міжнародній арені.

Зважаючи на викладене, вбачається за доцільне Службі безпеки України сприяти можливому розгортанню на базі Секретаріату ГУАМ в Україні технологічної складової Центру для організації навчального процесу, обміну інформацією тощо та віддаленого доступу визначених державних органів країн – членів ГУАМ. Питання фінансування роботи майбутнього Центру пропонується опрацювати в межах міжнародного співробітництва ГУАМ із США, Японією, ЄС тощо.

Зокрема, у межах майбутнього Центру можливий обмін даними щодо кіберінцидентів, розроблення тренінгових програм, а також програм підвищення професійного рівня співробітників органів країн – членів ГУАМ, які відповідають за забезпечення кібербезпеки тощо.

Як можливі напрями роботи Центру доцільно розглянути такі:

– проведення аналітичних досліджень та підготовка постійних (щомісяця, щокварталу тощо) публікацій щодо ситуації у сфері забезпечення кібербезпеки та протидії кіберзагрозам у країнах – членах ГУАМ;

– проведення кампаній із кібергігієни та кіберобізнаності (cyberawareness) у громадському середовищі країн – членів ГУАМ;

– розроблення методичних рекомендацій щодо здійснення об'єктами критичної інфраструктури захисту мереж та інфраструктур від несанкціонованого проникнення та кібератак;

– перепідготовка та підвищення кваліфікації співробітників профільних державних органів, до компетенції яких належать забезпечення кібербезпеки та протидія кіберзагрозам;

– розроблення та впровадження тренінгових програм для підготовки експертів команд реагування на кіберінциденти;

– обмін відкритою інформацією щодо кібератак / кіберінцидентів (ідентифікатори компрометації) на базі віртуальної платформи

Висновки. У процесі проведеного дослідження питань міжнародного співробітництва СБ України у сфері забезпечення кібербезпеки в межах міжнародних, зокрема й регіональних, організацій визначено основні чинники, які сприяють або можуть ускладнювати ефективність міжнародного співробітництва у сфері інформаційної безпеки та кібербезпеки.

Визначено завдання та перспективи розвитку Центру кібербезпеки Наукового-навчального інституту інформаційної безпеки та стратегічних комунікацій, що створений у складі Національної академії СБ України, який повинен функціонувати як системний центр з підготовки кадрів і забезпечення професійної сертифікації фахівців із кібербезпеки на державному рівні.

Запропоновано шляхи покращання міжнародної взаємодії на базі створення Регіонального центру ГУАМ у сфері кібербезпеки України, конкретні напрями його роботи, що сприятимуть зміцненню міжнародних контактів у межах НАТО, ЄС, Ради Європи, ОБСЄ, налагодженню механізмів обміну світовими практиками в галузі кібербезпеки та боротьби з кіберзлочинністю, покращанню іміджу ГУАМ на міжнародній арені.

Список використаних джерел

1. Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV : Закон України. URL: http://www.zakon2.rada.gov.ua/laws/show/2824-15 (дата звернення: 20.04.2021).

2. Климчук А. А., Панченко В. Н., Петров В. В. Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз. Київ, 2013. С. 123.

3. Budapest Convention, 2020 рік. URL: http://www.coe.int/en/web/cybercrime (дата звернення: 20.04.2021).

4. Budapest Convention, 2017 рік. URL: http://www.coe.int/en/web/cybercrime (дата звернення: 21.04.2021).

5. Щодо проекту Ради Європи «Cyber-East», н.с. 133, т. 2. 2019. С. 145–146.

6. Кримінальний процесуальний кодекс України. Київ, 2015. С. 11, 86–87.

7. Budapest Convention, 2019 рік. URL: http://www.coe.int/en/web/cybercrime (дата звернення: 21.04.2021).

8. Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines. Revised study and guidelines, 2018 рік. URL: http://www.coe.int/en/web/cybercrime (дата звернення: 20.04.2021).

International experience in the field of ensuring information security of person, society, state

Аннотация. В статье рассматриваются некоторые аспекты сотрудничества Службы безопасности Украины в сфере обеспечения кибербезопасности и противодействия киберугрозам с соответствующими органами стран – членов Организации за демократию и экономическое сотрудничество ГУАМ в формате Рабочей группы стран ГУАМ по вопросам кибербезопасности.

Определены основные факторы, которые на сегодняшний день способствуют или могут усложнять эффективность указанного сотрудничества. Предлагается для улучшения международного взаимодействия создание Регионального центра ГУАМ в Украине и конкретные направления его работы, которые помогут укрепить международные контакты, улучшить работу механизмов обмена мировыми практиками в сфере борьбы с киберпреступностью.

Ключевые слова: кибербезопасность, киберугрозы, Организация за демократию и экономическое сотрудничество ГУАМ, Региональный центр ГУАМ в сфере кибербезопасности, Рабочая группа ГУАМ по вопросам кибербезопасности.

Abstract. The article examines some aspects of cooperation between the Security Service of Ukraine and the relevant bodies of the member countries of the Organization for Democracy and Economic Cooperation GUAM in the field of cybersecurity and countering cyber threats in the format of the GUAM Countries Working Group on Cybersecurity.

The main factors that currently contribute or may complicate the effectiveness of this cooperation have been identified. It is proposed both the creation of a GUAM Regional Center in Ukraine and specific areas of its work to improve international cooperation, which will help strengthen international contacts as well as to improve the work of mechanisms for the exchange of world practices in the field of combating cybercrime.

Key words: cybersecurity, cyber threats, Organization for Democracy and Economic Cooperation GUAM, GUAM Regional Center for Cyber Security, GUAM Working Group on Cyber Security.