

## НАЦІОНАЛЬНА БЕЗПЕКА

**Василишин В.Ю.**

*студент,*

*Національна академія Служби безпеки України*

### **ДІЯЛЬНІСТЬ ПІДРОЗДІЛІВ СБ УКРАЇНИ В КОНТЕКСТІ ЗДІЙСНЕННЯ КОНТРРОЗВІДУВАЛЬНОГО ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ**

З розвитком суспільного життя в діяльності Служби безпеки України виникають нові виклики, які потребують швидкого реагування та попередження несприятливих наслідків для основ національної безпеки України. Не є виключенням інформаційна безпека держави. Адже будь-який державний орган має у своєму підпорядкуванні ресурси, заволодіння чи втручання в роботу яких завдає шкоду об'єктам критичної інфраструктури. Тому, серед основних завдань, які здійснює Служба безпеки України є контррозвідальне забезпечення інформаційної безпеки держави. Одним з підрозділів в системі СБ України за яким закріплені такі завдання є Департамент контррозвідального захисту інтересів держави у сфері інформаційної безпеки (далі – ДКІБ СБ України) та відділи у регіональних управліннях СБУ.

В межах своєї компетенції ДКІБ СБ України взаємодіючи з іншими підрозділами протидіє проведенню проти нашої держави спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, суверенітету і територіальної цілісності, кіберзагрозам, розповсюдженню інформації (зокрема в соціальних мережах), яка має на меті пропагувати тероризм та сепаратизм, тощо.

На сьогоднішній день одним з ключових завдань, які поставлені перед Службою безпеки України є реалізація комплексу заходів, що спрямовані на протидію гібридній війні з боку РФ в інформаційній сфері.

Як зазначає генерал-майор О.Климчук, начальник ДКІБ СБ України: гібридна агресія Російської Федерації щодо України є різноманітним поєднанням різноманітних комбінацій форм та методів негативного впливу, серед яких домінуючим напрямком є інформаційний та кібернетичний. Важливим аспектом негативного інформаційного впливу, що намагаються здійснювати російські спецслужби, є його спрямованість на руйнування української державності починаючи з базового рівня – історичної пам'яті та самоусвідомлення нації як такої. З цією метою російськими спецслужбами використовуються підконтрольні їм ЗМІ, інтернет-ресурси, групи у соцмережах, блогери, тролі та навіть поштові сервіси. Саме через цю розгалужену мережу не тільки збирається розвідальна інформація про

українських громадян, але й проводяться деструктивні пропагандистські інформаційні операції [1].

Соціальні мережі є серйозним інструментом завдяки якому іноземні спецслужби здійснюють спеціальні інформаційні операції, які мають на меті маніпулювати свідомістю громадян. Завдяки повному контролю над соцмережами «Вконтакте» та «Однокласники» російським спецслужбам відкрився доступ до приватної інформації громадян з різних куточків світу. Інтернет-ресурси перетворилися на канали дезінформації, поширенню антиукраїнського контенту та вербування нових прихильників «ЛДНР». Саме тому в травні 2017 року за ініціативою СБУ було прийнято рішення про блокування сайтів на території України, що дало змогу зменшити шкідливий вплив на інформаційний суверенітет України.

За даними СБУ у 2018 році вжито заходи превентивного впливу щодо 220 адміністраторів інтернет-спільнот, які поширювали в мережі матеріали деструктивного змісту на аудиторію понад 10 мільйонів інтернет-користувачів. Таким чином Служба не допустила скоєння злочинів, відповідальність за які передбачена Кримінальним кодексом України, а саме ст. 109 (дії спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади), ст. 110 (посягання на територіальну цілісність і недоторканість України) та ст. 258-3 (створення терористичної групи чи терористичної організації) [2].

Дуже важливою є протидія кібернетичним загрозам. Функціонує Ситуаційний центр забезпечення кібербезпеки СБУ (24/7), який здатний виявляти кіберзагрози та кібератаки, щоденно фіксує тисячі IP-адрес та інші дані інформаційних ресурсів, з яких здійснюються кібератаки на території України. Зараз фіксується збільшення як кількості кібератак, так і їх масштабності, що потребує відповідного реагування та дослідження. Основний напрямок хакерських атак спрямований на системи та об'єкти критичної інфраструктури нашої країни, правоохоронні органи, урядові та банківські установи. Співробітники ДКІБ СБ України встановили російське походження останніх масштабних кібератак, адже спецслужби РФ зробили Україну своєрідним майданчиком для відпрацювання хакерських атак на інші країни, зокрема на ЄС.

Крім цього російські спецслужби все частіше почали використовувати кібератаки як складові заходів деструктивного інформаційно-психологічного впливу для інспірування протестних настроїв та загострення суспільно-політичної обстановки в Україні.

Наразі Служба безпеки України здійснює контррозвідувальні, оперативно-розшукові та оперативно-технічні заходи з метою захисту інформаційної безпеки держави. Адже, інформація – найцінніший ресурс в умовах гібридної війни, тому вкрай необхідні законодавчо закріплені елементи для її захисту. Функціонування Ситуаційного центру забезпечення кібербезпеки СБУ та заходи стосовно протидії спеціальним інформаційним операціям безумовно дають позитивні результати. Однак, варто завжди бути напоготові до нових деструктивних явищ проти інформаційної безпеки не лише України, але і всього світового співтовариства. Про це свідчать постійні атаки хакерських

угруповань на об'єкти критичної інфраструктури, розповсюдження шкідливого програмного забезпечення через шифрувальника файлів (в пам'яті одразу згадується Petya.A, який використовував мережеву вразливість MS17-010, внаслідок експлуатації якої на інфікований ПК встановлювався набір скриптів, що використовували зловмисники для запуску вказаного шифрувальника файлів) та інформаційний тероризм в глобальній мережі інтернет.

### **Список використаних джерел:**

1. Климчук О.В. Інформаційна та кібербезпека у сучасному світі: досвід СБУ [Електронний ресурс] / О.В. Климчук – Режим доступу: <https://ua-news.liga.net/politics/opinion/informatsiyna-ta-kiberbezpeka-v-suchasnomu-sviti-dosvid-sbu>

2. Служба безпеки України активно протидіє агресії РФ в інформаційній сфері / офіційний веб-сайт Служби безпеки України – Режим доступу: <https://ssu.gov.ua/ua/news/1/category/320/view/5545#.OvMcug7h.dpbs>

### **Левчук О.В.**

*кандидат економічних наук, доцент,  
Національний університет оборони України  
імені Івана Черняхівського*

## **ЗАЛУЧЕННЯ ІННОВАЦІЙ ЯК ВАЖЛИВИЙ ФАКТОР РОЗВИТКУ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ**

На сьогоднішній день проблема економічної безпеки зачіпає інтереси багатьох країн. Світовий досвід переконливо доводить, що збиток економічним інтересам можна надати різноманітними спробами: порушенням нормального стану міжнародної торгівлі (застосування ембарго, введення надмірних кількісних і тарифних обмежень, штучне підвищення або зниження цін на ті на інші товари), створенням перепон на шляху міжнародного руху технологій тощо.

В основу системи інтенсифікації виробництва покладено розвиток світових ринків товарів, послуг, праці, капіталу й технологій через скоординовану інноваційну політику. Економічна інноваційна політика – новий рівень інтернаціоналізації та міжнародної економічної інтеграції, що характеризується інтенсифікацією і новою якістю внутрішніх міжнародних зв'язків у планетарних масштабах [2].

Метою даного дослідження є аналіз сучасного стану зовнішньоекономічної діяльності в поєднанні з сучасними інноваційними процесами.

Стрімка інтелектуалізація виробництва, ринку й зовнішньоекономічної діяльності викликані небаченими темпами росту обсягів і масштабу інновацій, які докорінно змінюють соціально-економічну структуру суспільства та виробничих відносин.

Протягом тривалого часу національні виробники не відчували достатньої внутрішньої мотивації застосування інновацій, що давало можливість іноземним