к.т.н. Козубцова Л.М. (ВІТІ ім. Героїв Крут)
к.т.н. Бескровний О.І. (ВІТІ ім. Героїв Крут)
д.п.н., к.т.н. Козубцов І.М. (ВІТІ ім. Героїв Крут)

ГІБРИДНА ПОБУДОВА СИСТЕМИ КІБЕРБЕЗПЕКИ НА ЗАСАДАХ ВІЙСЬКОВО-ЦИВІЛЬНОГО СПІВРОБІТНИЦТВА

З початком повномасштабної військової агресії Російської Федерації проти України, Державні органи та формування сектору безпеки і оборони України зіткнулися з веденням гібридної війни проти себе із застосуванням кіберпростору. Порушення функціонування українського сегменту кіберпростору змусило переглянути існуючі підходи до побудова системи кібербезпеки і таким чином забезпечити гарантовану безпеку держави.

Аналіз досліджень показав, що дана проблематика привернула увагу зарубіжних та вітчизняних науковців, однак предмет їх дослідження не охопив питання функціонування кіберпростору Державних органів та формування сектору безпеки і оборони України в умовах гібридної війни.

Мета доповіді. Обґрунтувати підстави створення гібридної системи кібербезпеки Державних органів та формування сектору безпеки і оборони України на засадах військово-цивільного співробітництва. Для досягнення мети поставлено такі задачі: 1. Проаналізувати сучасний стан досліджень та публікацій. 2. Обґрунтувати підстави створення гібридної системи кібербезпеки Державних органів та формування сектору безпеки і оборони України на засадах військово-цивільного співробітництва.

3. Обговорити адміністративно-правові засади гібридного військово-цивільного співробітництва Державних органів та формування сектору безпеки і оборони України.

Результати дослідження. Пропонується можливість організувати функціонування та взаємодію Державних органів та формування сектору безпеки і оборони України з приватним сектором для нейтралізації кіберзагроз на підставі Статті 10. «Державно-приватна взаємодія у сфері кібербезпеки» Закону України «Про основні засади забезпечення кібербезпеки України», де визначено:

пункт 1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

підпункт 1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

підпункт 3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

підпункт 4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;

підпункт 6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

підпункт 11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

Враховуючи вище зазначене, небайдужими адміністраторами було створено телеграм-канал «Кібер Армія», «Stop Russian Channel MRIYA». До професіоналів сфери ІТ долучилось понад 250 тисяч активних учасників звичайних людей для активних дій у кіберпросторі. Адміністратори періодично і за результатами обстановки в кіберпросторі формували дозовані завдання небайдужими фахівцями в галузі ІТ та кібербезпеки, а саме блокування інтернет ресурсів, що поширювали інформацію про насилля, шляхом подачі відповідних заявок адміністраторам відповідних ресурсів; реалізація активних заходів впливу на порушення правильності функціонування об'єктів критичної інформаційної інфраструктури РФ та Республіки Білорусь.

Таким чином, високу ефективність у протистояння гібридній війні РФ та нейтралізації кіберзагроз Державним органам та формуванням сектору безпеки і оборони України проявили саморганізовані гібридні підрозділи військо-цивільного співробітництва.