3. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року URL. https://zakon.rada.gov.ua/laws/show/995_199#Text.

4. Природа та війна: як військове вторгнення Росії впливає на довкілля України URL.https://ecoaction.org.ua/pryroda-ta-vijna.html?gclid=EAIaIQobChMI6Zfyn_nB_gIVhxh7Ch2B4gCNEAAYASAAEgKItfD_BwE.

Сокол Денис Олександрович
студент 201 н. г.
навчально-наукового інституту № 2
Національної академії внутрішніх справ

Науковий керівник:
Волошин Олексій Гнатович,
старший викладач кафедри
криміналістичного
забезпечення та судових експертиз
навчально-наукового інституту № 2
Національної академії внутрішніх справ

ПОНЯТТЯ, КЛАСИФІКАЦІЯ І ВИДИ КІБЕРЗЛОЧИНІВ В УКРАЇНІ В ПЕРІОД ПОВНОМАСШТАБНОЇ ВІЙНИ ДЕРЖАВИ-АГРЕСОРА

Російсько-українська війна поставила питання безпеки держави і суспільства на якісно новий рівень. Кібербезпека та боротьба з кіберзлочинністю в умовах воєнного стану XXI століття – це одні з найбільш важливих питань особливо в нашій країні, коли протистояння двох сторін переходить в кібергібридну війну. Операції з якими потребують глибокого аналізу, розробок та впровадження високотехнологічних рішень з метою запобігання та викриття кіберзагроз в цій галузі. Інформаційна та економічна безпека допомагають забезпечити функціонування держави, захистити інтереси нації та зберегти стабільність у складних умовах військового конфлікту.

Згідно з Рішенням ради національної безпеки і оборони України “Про План реалізації Стратегії кібербезпеки України”, яке уведене в дію Указом Президента України від 1 лютого 2022 року № 37/2022, кіберпростір визначено як один із ключових елементів воєнних дій. Основою кібероборони визначено кібервійська, які повинні забезпечувати ефективний захист критичної інформаційної

інфраструктури, державних інформаційних ресурсів та інформації. Також цим нормативним документом визначено завершення до 2025 року імплементації в законодавство України положень Конвенції про кіберзлочинність [1].

Нині у вітчизняній практиці термін «кіберзлочинність» вживається разом із терміном «комп'ютерна злочинність», під яким зазвичай розуміються злочини з допомогою комп'ютерної інформації. Термін «кіберзлочинність» зобов'язаний своєю появою виникнення та розвитку індустрії інформаційних та комп'ютерних технологій, яка поступово проникла у всі сфери життя світової спільноти.

У законі України "Про основні засади забезпечення кібербезпеки України" поняття кібербезпеки визначається як - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2].

Водночас поряд з наведеним терміном, вище зазначене національне законодавство передбачає також поняття "індикаторів кіберзагроз", "інформацію про інцидент кібербезпеки", "кіберінцидент", "кібератаку", "кібербезпеку", "кіберзагрозу", "кіберзахист", "кіберзлочинність", "кібероборону", "кіберрозвідку, "кіберпростір", "кіберрозвідка", "кібертероризм" та, зрештою, "кібершпигунство".

Наразі найпоширеніша класифікація кіберзлочинів базується на структурі Конвенції Ради Європи про кіберзлочинність Кіберзлочини можна класифікувати відповідно до їхньої мети, виконавця та способу вчинення.. Ця класифікація наразі слугує "еталоном", оскільки існуючі міжнародні, регіональні документи та наукові практики використовують цю класифікацію.

Умови збройного конфлікту суттєво збільшують загрози для кібербезпеки держави. Кібератаки можуть бути використані в якості зброї, яка наносить значну шкоду як військовим, так і цивільним об'єктам.

Умови збройного конфлікту роблять кібератаки ще більш небезпечними, оскільки їх метою може бути завдання шкоди об'єктам інфраструктури, комунікацій, електронної системи управління тощо. Можна виділити наступнівиди кібератак, які є найбільш характерними під час збройного конфлікту. [4 ст. 7]

DDoS атаки: Полягають у перевантаженні цільового сервера запитами, що призводить до відмови в обслуговуванні. Умови збройного конфлікту можуть призвести до масштабних DDoS-атак на важливі об'єкти. [4, с. 7]

Шкідливе програмне забезпечення та віруси: Зловмисний код може використовуватися для руйнування або злому інформаційних систем. У разі збройного конфлікту, це може стати інструментом руйнування інфраструктури.

Фішинг та соціальна інженерія: Шахраї можуть використовувати соціальні мережі та фішингові атаки для отримання доступу до конфіденційної інформації та керівництва держави. [4, с. 7]

Кібершпигунство: Держави або хакерські групи можуть використовувати кібершпигунство для здобуття важливих розвідувальних даних та секретів [4, с. 7]

Враховуючи викладені обставини, можна підсумувати, що в умовах повномасштабної російської-української війни кібератаки на об'єкти критичної інфраструктури, державні інформаційні ресурси розглядаються, як одні із сучасних методів ведення війни та тероризму. Аналіз законодавства та практики його застосування, дозволяє визначати проблему кібератак у сфері інформаційного простору аналогічно до наслідків військових дій. З розвитком сучасних технологій та впровадження їх в складову держави кібероборона, що включає в себе сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії, також стискається з стрімким розвитком та вдосконалення ключових видів атак, які становлять загрозу для кібербезпеки держави та її кіберпростору, включаючи кібератаки, кібершпигунство та кіберсаботаж.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 01.02.2022 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text.

2.Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

3.Бабійчук В.С. Кібертероризм та протидія йому. Молодий вчений. 2019. № 4 (68). Ст. 103–107. URL: https://doi.org/10.32839/2304-5809/2019-4-68-24.

4. Савченко В.А. Забезпечення стійкості кібероборони держави в умовах збройного конфлікту. Сучасний захист інформації. 2023. №3(55). Ст. 6–11. URL: https://doi.org/10.31673/2409-7292.2023.030001.