УДК 004.9:519.716

М. Л. Тюльпін

КІБЕРБЕЗПЕКА В РЕАЛІЯХ ВІЙСЬКОВОГО ЧАСУ

Вінницький національний технічний університет

Анотація

Питання захисту від кібератак та посилення можливостей інформаційної безпеки держави та її інформаційного простору актуальна вимога в реаліях військового часу.

Ключові слова: Україна, кібербезпека, кіберзахист, кібератака, кіберзагрози, інформаційна безпека, війна.

Abstract

The issue of protection against cyberattacks and the strengthening of information security is an urgent requirement in the realities of war.

Keywords: Ukraine, cyber security, cyber defense, cyber attack, cyber threats, information security, war.

Вступ

«*Хто володіє інформацією,*
той володіє світом»
(Натан Ротшильд)

Наше життя стає все більш залежним від комп'ютерних систем, а кібертехнології стають дедалі складнішими. Полем битви 21 сторіччя стає також і кіберпростір. Усе, починаючи від зламу паролей, викрадення даних банківських карт і до зламу потужних інформаційних систем банків, кібератаки можуть набувати безліч варіацій. Це підштовхує фахівців винаходити нові способи кіберзахисту, а уряди держав спонукає вірно розставляти пріоритети. Оскільки кібервійна не має територіальних обмежень, забезпечення кібербезпеки також вимагатиме прицільної уваги міжнародних співтовариств.

Аналізуючи сучасні дослідження та моделі протидії кіберзагрозам можна зробити висновок, що кількість загроз стрімко зростає. Так дослідники з компанії «Check Point» виявили, що кількість кібератак зростає на 50% із року в рік [1], відповідно змінюються моделі протидії атакам в залежності від розвитку технічного оснащення нападника та у відповідності до кількості залучених нападником людських ресурсів [2].

Напад Росії на Україну та початок повномасштабної війни поставив перед кібербезпекою нові завдання. Велика кількість населення України змушена була покинути свої домівки, завдяки чому змінилося їх інформаційно-комунікаційне оточення. В результаті основним джерелом інформації став Інтернет. Однак саме Інтернет заполонила велика кількість російських пропагандистів різного гатунку. Тому активна протидія фейковому впливу на населення України стає сьогодні основним напрямом забезпечення кібернетичної безпеки. Також важливим напрямком діяльності є підвищення ефективності комунікації із населення розвинених країн, які надають Україну так необхідну нам технічну та економічну допомогу.

Саме на противагу цим викликам і маємо політичні, економічні і соціальні зусилля з посилення кіберстійкості, які докладає держава задля розвитку національних можливостей з кібербезпеки, котре потребує комплексного вирішення і вимагає скоординованих дій на національному та регіональному рівнях [3].

Метою роботи є аналіз сучасного стану кібернетичної безпеки нашої країни, висвітлення важливості кіберзахисту в реаліях військового часу.

Результати дослідження

Проблематика захисту від кібератак існує давно. Ще декілька років назад питання посиленої уваги до кібербезпеки вже «підіймав» журнал «Захист інформації» [3], де наголошував на тому, що Україна

має докладати більше зусиль для запровадження захисту критичної інфраструктури. А також зазначалась необхідність у нарощуванні кібернетичного потенціалу з метою запобігання, підготовки, реагування та відновлення інцидентів на органи влади, приватного сектора та громадянського суспільства.

Актуальність цього питання у сьогоденних реаліях нині взагалі не викликає сумнівів. По даним сучасного видавництва «The Page» [4] з початку війни Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації та громадян. Це сигналізує про те, що в нашій державі існує гостра проблема кіберзахисту.

Також, підкреслюючи вагомість проблематики кібербезпеки, Президентом України був підписаний указ «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [5], де зазначаються актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію кіберзагрозам, дезінформації, насамперед держави-агресора, захист прав осіб на інформацію та захист персональних даних.

Серії серйозних кібератак Кремля на Україну напередодні та на початку війни, говорить про те, що Росія готувалася до цього планово та заздалегідь. Лише за три дні конфлікту наприкінці лютого 2022р. дослідники «Check Point Research» (CPR) відзначили зростання на 196% кібератак на урядовий та військовий сектор України.

У період війни пріоритетними цілями захисту окрім безпеки критичної інфраструктури має бути захищеність інформаційного простору. Також важливий бізнес має бути готовий протидіяти викликам інформаційної безпеки. Плідне використання кібератак, кампаній з дезінформації, криптовалют означає, що ця війна відрізняється від усіх, які Світ бачив раніше. Як бачимо з результатів дослідження [6] рис. 1 у 2022 році найбільш атакованим сектором є освіта, а атаки на охорона здоров'я зросли на 60% порівняно з минулим роком. На другому місці атаки на державну та військова сфери, що на 20 % більше, ніж за той самий період минулого року.

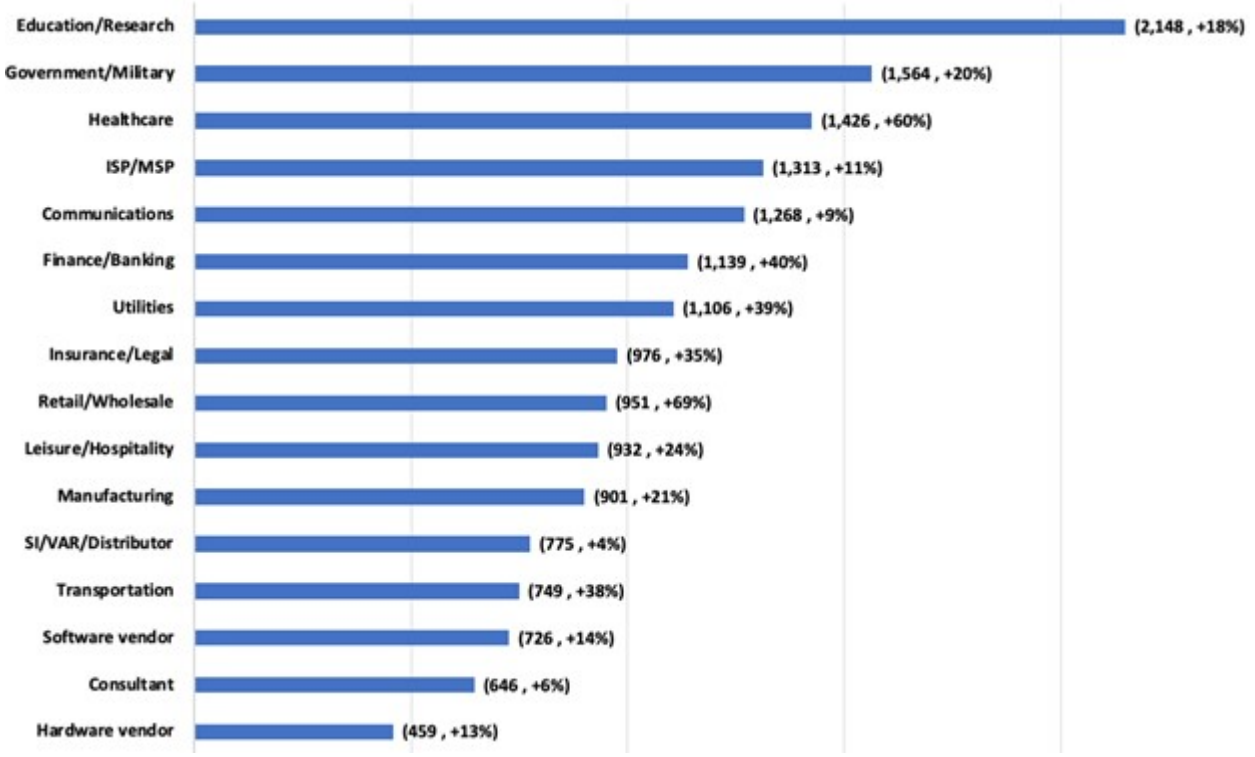

Рис. 1 Середньотижнева кількість атак на організації за галузями у 2022році у порівнянні з 2021 роком.

Наша держава може витратити величезну кількість коштів на висококласні наступальні можливості та захист своїх власних найважливіших військових та інших активів національної безпеки, але тим не менш захист від кібератак в реаліях військового часу є невідкладною вимогою.

Вторгнення Росії в Україну похитнуло світ і віру у безпеку. І хоча Україна завжди була прихильником кібернорм, в реаліях військового часу Україні не потрібно їх дотримуватися по відношенню до

свого нападника (з-но винятку з тексту Статуту ООН [7] - коли застосування сили є необхідним для індивідуальної або колективної самооборони у відповідь на «збройний напад».

Україна реалізувала і продовжує посилювати комплекс заходів для вирішення стратегічних, політичних та технічних питань задля готовності забезпечувати кібербезпеку і відбивати відкриту агресію в кіберпросторі. Тим не менш необхідно приділяти увагу удосконаленню національної стратегії кіберзахисту, висвітлювати інформацію про кіберзагрози у засобах масової інформації, формувати культуру кіберзахисту в державі.

Висновки

В доповіді показано, що тема кібербезпеки в реаліях військового часу є над важливою. Кіберзлочинці на теренах війни відточують свою майстерність, а сучасні інформаційні технології надають можливість зірвати, затримати, дратувати, пограбувати, викрасти, шпигувати за противником і впливати на нього. Новітні техніко-інформаційні можливості є обов'язковими для всіх сучасних військових систем. Тому вони мають місце у військовому конфлікті та поза ним, і наша держава має бути готова, як до кіберзахисту так і до кібератак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Check Point Research: Cyber Attacks Increased 50% Year over Year. URL: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year.
2. Нікіфорова Л.О., Яремчук Ю.Є., Шиян А.А. Моделювання вибору оптимального методу протидії загрозам інформаційній безпеці. Реєстрація, зберігання і обробка даних. 2014. Т.16, №4. С.28-33.
3. Трофіменко О. Г., Прокоп Ю. В., Логінова Н. І.,. Задерейко О. В Кібербезпека України: аналіз сучасного стану. Захист інформації. Том 21. 2019. № 3. С. 150-157.
4. Янковський О. Як забезпечити кібербезпеку в умовах воєнного часу. URL: https://thepage.ua/ua/experts/yak-zabezpechiti-kiberbezpeku-v-umovah-voyennogo-chasu.
5. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки».
6. Check Point Research: Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends. URL: https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks.
7. Статут Організації Об'єднаних Націй/Розділ VII/Стаття 51. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf.

Тюльпін Михайло Леонідович — студент групи 1КІТС-22М, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: mtyulpin@gmail.com

Науковий керівник: ***Шиян Анатолій Антонович*** — канд. Фіз.-мат. наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця

Tiulpin Myhailo – Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: mtyulpin@gmail.com

Supervisor: ***Shyian Anatolii*** — PhD (Phys. and Math.), Associate Professor, Associate Professor of the Chair Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia