Красненко Вікторія Костянтинівна
курсант 201 навчальної групи ННІ № 3 НАВС, капрал поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

СУЧАСНІ ВИКЛИКИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

У сучасних умовах зафіксовано зростання кількості кібератак, що стає наслідком триваючої кібервійни та збільшення загрози з боку російських хакерів. Тому забезпечення ефективного кіберзахисту стає одним із найактуальніших завдань, оскільки у багатьох сучасних організацій різних галузей діяльності всю інформацію все частіше зберігають у цифровій або електронній формі на окремих комп'ютерах чи інших пристроях для зберігання даних.

Незважаючи на те, що проблеми кібербезпеки в Україні в умовах воєнного стану були предметом наукових дискусій у роботах Корнейка О.В., Корчевського М.В., Кудінова В.А., Хахновського В.Г., Ярового К.В. та інших, насьогодні, зазначене питання не втрачає своєї актуальності.

Слід зазначити, що поняття інформаційної безпеки є ще одним методом визначення безпеки даних, який включає в себе конфіденційність, цілісність та доступність даних. Інформаційна безпека України є важливою складовою національної безпеки і забезпечує захист державного суверенітету, територіальної цілісності, демократичного конституційного ладу, а також інших важливих інтересів людини, суспільства і держави. Вона включає в себе забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації, а також доступ до достовірної та об'єктивної інформації [2, с. 106]. Крім того, існує ефективна система захисту та протидії нанесенню шкоди через поширення негативних інформаційних впливів, включаючи скоординоване поширення недостовірної інформації, деструктивну пропаганду та інші інформаційні операції, а також несанкціоноване розповсюдження, використання та порушення цілісності інформації з обмеженим доступом. Більшість сучасних бізнес-даних зберігаються в електронному вигляді на серверах, настільних комп'ютерах, ноутбуках або в мережі Інтернеті, в той час як десять років тому конфіденційна інформація зберігалася в архівах та кабінетах перед тим, як бути перенесеною в Інтернет.

Останнім часом велика увага дослідників приділяється кібербезпеці та її різноманітним аспектам. Проте, багато ще залишається невідомим у зв'язку зі швидкими темпами розвитку електронних технологій та суспільства загалом. Нові можливості інформаційного впливу на суспільство породжують нові загрози безпеці, що вимагають постійного оновлення та удосконалення систем захисту [2, с. 106].

Тому на нашу думку, концепція кібербезпеки потребує перегляду в контексті стрімких змін у світі інформації та домінуючих тенденцій розвитку глобального суспільства, яке все більше орієнтується на «інформаційні» виміри.

Водночас аналіз чинного законодавства вказує на те, що існує ряд недоліків щодо регулювання питання кібербезпеки (оборони), які потребують негайного формування пропозиції щодо шляхів вирішення існуючих проблем з урахуванням європейської інтеграції.

У цьому контексті слушної є думка Черниш Ю.О. та Мальцевої І.Р. про те, що дані зараз здебільшого зберігаються в електронному або цифровому форматі, тому найбільше уваги приділяється кібербезпеці. Так звані кібератаки від комп'ютерних вірусів і хакерства стали серйозною загрозою для комп'ютерних систем і мереж у всьому світі. Сучасні організації повинні надсерйозно сприймати ці загрози та інвестувати час і ресурси, необхідні для захисту своїх цифрових активів, в кібербезпеку, або ризикувати потенційно шкідливими системними зломами та збоями [3, с. 94].

У висновку слід підкреслити, що для вирішення проблематики інформаційної безпеки необхідна комплексна стратегія, яка охоплює різні аспекти цього питання. Зокрема, важливо здійснювати постійний моніторинг та аналіз загроз, впроваджувати сучасні технології захисту даних, підвищувати обізнаність персоналу з питань кібербезпеки, а також співпрацювати з іншими країнами та міжнародними організаціями для обміну досвідом та взаємної підтримки.

Крім цього, важливо також регулярно оновлювати законодавство та нормативно-правову базу у сфері інформаційної безпеки, щоб відповідати новим викликам та загрозам. Тільки через комплексний підхід та спільні зусилля різних сторін можна досягти успішного вирішення проблем інформаційної безпеки і забезпечити стабільний розвиток суспільства в умовах цифрової епохи.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/ show/2163-19#Text.

2. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

3. Черниш Ю. О., Мальцева І. Р, Штонда Р. М. Аналіз деяких кіберзагроз в умовах війни: Електронне фахове наукове видання. Кібербезпека: освіта, наука, техніка, 4 (16), 2023. С. 37-44.