

УДК 378.016: 329.09.5(477)

Баєва Л.В.¹, Носенко Я.Д.²

¹канд. юрид. наук, доц. НУ «Запорізька політехніка»

²студ. гр. Ю-319 НУ «Запорізька політехніка»

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, держави. Сьогодні ми все більше й більше використовуємо їх у своїй діяльності, жертвами кібератак можуть стати не лише люди, але підприємства, критична інфраструктура та цілі держави. За ефективністю та наслідками застосування кіберзброї а саме такий термін все частіше використовують ІТ спеціалісти можна прирівняти до зброї масового ураження.

Кібербезпека включає в себе захист інформації, але не обмежується лише нею. Це захист від вірусів, хакерських атак, підробки даних, які можуть не тільки видалити/вкрасти дані, але і вплинути на роботу і продуктивність співробітників, використовувати інформацію проти людини або структури, а також зупинити виробництво. Кібербезпека сьогодні відповідає за три чинники: системи, процеси, люди.

Стрімке впровадження інформаційних технологій у всі сфери життя, глобалізація інформаційних відносин зумовлюють світову тенденцію до перенесення протиправної діяльності у кібернетичний простір. сьогодні комп'ютерна злочинність, чи кіберзлочинність, для якої не існує державних кордонів, загрожує не лише правам та майну громадян, а й посягає на національні інтереси. Спостерігається висока вразливість кібернетичного простору перед кібератаками, діяльністю злочинних угруповань, хакерів груп та осіб, допущених до роботи із системами в порядку здійснення службової діяльності (інсайдерів). Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів,

яким може бути завдано збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує і задає інформаційний обмін між всіма елементами соціуму.

Запровадження закону України «Про основні засади забезпечення кібербезпеки України», визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Закон також дає чіткі визначення понять «кібербезпека», а саме кібербезпека – 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. Інформаційна безпека є невід’ємною частиною загальної проблеми інформаційного забезпечення як людини, так держави і суспільства в цілому. Вона направлена на захист суб’єктів інформаційних ресурсів.

Побудова усталеної системи інформаційної безпеки держави в умовах глобалізації та розвитку інформаційних технологій і телекомунікаційних систем потребує з’ясування системоутворювальних основ і базових принципів системи забезпечення кібербезпеки як найважливішої складової інформаційної безпеки України. На підставі аналізу наукових публікацій можна стверджувати, що дослідження проблеми забезпечення інформаційної безпеки відбувається, як правило, за двома основними напрямками – інформаційно-психологічному, спрямованому на захист свідомості від негативного інформаційного впливу та інформаційно-технічному, в якому основним об’єктом захисту є інформаційні ресурси в інформаційно-телекомунікаційних системах.

Отже, інформаційну безпеку держави можна трактувати як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.