Питання підтримання інформаційної безпеки (ІБ) перебуває сьогодні для України на одному рівні з захистом суверенітету й територіальної цілісності, гарантуванням її економічної безпеки. Рівень ІБ безпосередньо впливає на стан політичної, економічної, оборонної та інших складових національної безпеки Української держави, оскільки реалізація інформаційних загроз – це заподіяння шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо.

Поява нових загроз обумовила політичну необхідність контролю (регулювання) кіберпростору, прийняття відповідних концепцій і норм. Пріоритетність питань кібербезпеки для подальшого розвитку Інтернету визнана на Всесвітньому саміті з розвитку інформаційного суспільства (ІС).

<…> Тенденції вибору Україною шляху інтеграції у світове співтовариство та перспективи вступу до Європейського Союзу зумовлюють необхідність участі в процесах створення й використання єдиних принципів формування ІС, законодавчого регулювання та керування інформаційною сферою.

Такі досягнення України, як вступ до СОТ і зростання міжнародного авторитету вітчизняних ІТ-фірм, демонструють наявність потенціалу розвитку та зміцнення економіки країни у XXI ст., коли ІТ стали основою розвитку нового суспільства – інформаційного.

<…> Для України, яка прагне ввійти до європейського співтовариства, особливо важливим є приведення чинного законодавства до європейських стандартів, що передбачає прийняття нових законів, удосконалення й доопрацювання чинної нормативно-правової бази. Існує також необхідність у визначенні або створенні координуючого органу з питань нормативно-правового забезпечення регулювання відносин у кіберпросторі, зокрема гарантування інформаційної безпеки країни, який акумулював би пропозиції різних органів державної влади та громадських інституцій у справі вироблення інформаційної політики для України.

Якщо в попередні десятиліття державна політика у сфері гарантування інформаційної безпеки була орієнтована на загрози, які в кібер-просторі можуть бути спричинені терористичними та кримінальними угрупуваннями (спецслужби очікували на інспіровані катастрофи потягів і літаків, техногенних аварій), то тепер акценти у сфері міжнародної безпеки змістились у бік повномасштабної системи захисту інформації. На сучасному етапі суспільного розвитку головними суперниками визнаються не хакери-одинаки, а спеціально створені державами служби. Матеріальні збитки від викраденої інформації оцінюються в мільярди доларів США.

<…> Стислий аналіз чинного законодавства, яке охоплює тільки деякі аспекти взаємовідносин у кіберпросторі, показує відсутність комплексної та системної законодавчої підтримки діяльності державних органів у сфері

ведення інформаційного протиборства. Забезпечити відповідні комплексність і системність може допомогти розробка концепції інформаційного протиборства у кіберпросторі.

Ураховуючи провідну роль інформатизації в економіці України та відповідне її розвиткові стрімке зростання кількості кримінальних злочинів у кіберпросторі, особливої актуальності нині набуває внесення змін і доповнень до чинного законодавства та відомчих нормативних актів, які повинні забезпечити адекватне функціонування інформаційних систем і мереж, створити умови для мінімізації, своєчасного виявлення та запобігання кібер-злочинам.

Адекватним заходом реагування за таких умов має бути застосування новітніх розробок інструментарію, засобів і систем для виявлення та протидії зовнішнім інформаційним загрозам національній безпеці України, а також для захисту інформації та інформаційних систем і мереж від кіберзагроз ***(Мєзєнцева Н. До питання нормативно-правового регулювання взаємовідносин у кіберпросторі в контексті підтримання безпеки України в інформаційній сфері // Наука і оборона. – 2012. – № 1. – С. 29–31, 33).***