Юдкова К. В.
викладач ФСП НТУУ «КПІ»

ПРАВОВА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розробка дієвого механізму вирішення питань забезпечення інформаційної безпеки за допомогою методу соціально-правового моделювання є комплексною міждисциплінарною проблемою, що синтетично поєднує сфери досліджень як соціально-правових, так і технічних наук. Впровадження досліджень загроз інформаційної безпеки та розробка засобів їх запобігання за допомогою правової моделі інформаційної безпеки значно розширить можливості органів державної влади щодо дотримання правопорядку та забезпечення національної безпеки, а також знизить затрати організаційно-технологічних ресурсів, що надаються для забезпечення інформаційної безпеки.

Забезпечення стану дотримання безпеки інформації є одним із превалюючих завдань держави у процесі побудови дієвої системи забезпечення загального механізму не порушення прав та свобод громадян, державних та громадських інтересів. Відповідно до положень Указу Президента України «Про Доктрину інформаційної безпеки України» від 08.07.2009, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки [1].

Тобто, інформаційна безпека є перманентним процесом сталого розвитку. Таким чином, правова модель інформаційної безпеки, для забезпечення досягнення її основних цілей, обов’язково має бути динамічною та гнучкою, мати можливість розвиватися та здатність до перебудови та зміни власних структурних елементів.

Станом захищеності інформацій є такий її стан, коли зберігаються три основні її характеристики:

- конфіденційність;
- цілісність;
- доступність.

Правова модель інформаційної безпеки – це таке відображення суспільно-правових та організаційно-технічних процесів, яке повністю або за основними характеристиками відповідає реальним правовідносинам та при взаємодії із зовнішніми негативними факторами повною мірою відображає наслідки такої взаємодії, що робить можливим впровадження дієвого механізму запобігання.

Як згадувалося вище, організація забезпечення інформаційної безпеки ґрунтується на глибокому аналізі негативних наслідків. Задля здійснення аналізу негативних наслідків обов'язковою є ідентифікація можливих джерел загроз, факторів, що сприяють їх прояву, визначення актуальних загроз

інформаційної безпеки. Таким чином моделювання доцільно проводити, визначивши:

1) джерела загроз;
2) рівень інформаційного імунітету об’єкта загрози;
3) загрози;
4) можливі наслідки.

Крім того, побудова моделі інформаційної безпеки передбачає не тільки виявлення загроз та їх аналіз з метою виявлення наслідків та оцінки можливих збитків в разі їх реалізації. Але й слугує засобом перевірки розроблюваних методів та способів захисту інформації і прогнозування виникнення нових загроз з метою подальшого їх запобігання.

Побудова моделі з орієнтацією на правову основу, обумовлена тим, що саме право є універсальним регулятором суспільних відносин, крім того, відповідна правова культура виконує функції профілактики загроз і більш серйозних наслідків.

Не менш важливим є і той факт, що інформація є не тільки абстрактною філософської категорією, але й ресурсом. Тобто об’єктом суспільних відносин і, як наслідок, об’єктом правового регулювання. Застосування методу моделювання слід розглядати як процес об'єктивно обумовлений, який має на меті розробити наукове забезпечення для концепції інформаційної безпеки як складової національної безпеки і шляхом впровадження нових інформаційних технологій підвищити результативність діяльності щодо її реалізації.

На підставі вищенаведеного можна надати визначення правової моделі інформаційної безпеки - кількісно-якісний опис можливого варіанту забезпечення системи безпеки, з обов'язковим визначенням її цілей і завдань, оцінкою рівня інформаційного імунітету, можливих загроз, а також розробкою правових механізмів підвищення захищеності системи та її здатності до самозахисту від цих загроз.

Недостатність та фрагментарність законодавчої та нормативної бази створює всі умови для неможливості застосування комплексного підходу до забезпечення інформаційної безпеки. Аналіз результатів роботи із комплексною правовою моделлю інформаційної безпеки є достатнім обґрунтуванням розробки низки нормативно-правових та нормативних актів для врегулювання суспільних відносин в сфері інформаційної безпеки та побудови чіткої організаційно-сприятливої системи відповідних державних органів та установ на всіх рівнях державної влади.

Таким чином, комплексна правова модель інформаційної безпеки забезпечить можливість превентивної боротьби з існуючими загрозами, передбачення та недопущення виникнення нових загроз або дієве запобігання їх руйнівних наслідків.

Список використаних джерел

1. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.2009 № 514/2009 // Офіційний вісник Президента України 2009 р., № 20, стор. 18, стаття 677