національну безпеку і оборону. Тому через відсутність обґрунтованих класифікаторів та методик визначення шкоди національній безпеці, посадовці дуже успішно користуються прикриванням таких відомостей шляхом їх засекречення [4].

Ще однією, досить банальною причиною порушення режиму секретності є недостатнє фінансування режимно-секретних органів (РСО) органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, які провадять діяльність пов'язану з державною таємницею. Так через відсутність належного обладнання приміщень РСО, відсутність сейфів, відомості, що містять державну таємницю, можуть потрапити до осіб, що не мають належного допуску до них та можуть бути розголошені.

Отже слід сказати, що в Україні правовому регулюванню захисту державної таємниці приділяється велике значення, однак існує ряд спірних питань, які створюють перешкоди для нормального функціонування системи охорони державної таємниці, вирішення яких позитивно вплинуло б на рівень забезпечення державної безпеки у цій сфері.

Список використаних джерел:

1. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. // Відомості Верховної Ради України. – 2003. – № 39.

2. Закон України «Про державну таємницю» : від 21 січня 1994 р. // Відомості Верховної Ради України. – 1994. – № 16.

3. Благородний А.М. Адміністративна відповідальність за порушення законодавства про державну таємницю : дис. … канд. юрид. наук. – К., 2006. – 200 с.

4. Захаров Є. Які відомості становлять державну таємницю в Україні? / Є. Захаров, І. Рапп. – http:/www.khpg.org./index.php?id=1141143392

Дем'янчук Ю.В.

кандидат юридичних наук,

Білоцерківський гуманітарно-педагогічний коледж

АКТУАЛЬНІ ПРОБЛЕМИ ПРАВОВОГО МОДЕЛЮВАННЯ 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. Упровадження досліджень загроз інформаційній

безпеці та розробка засобів їх запобігання за допомогою правової моделі інформаційної безпеки значно розширять можливості органів державної влади щодо дотримання правопорядку та забезпечення національної безпеки, а також знизять затрати організаційно-технологічних ресурсів, що надаються для забезпечення інформаційної безпеки.

Найбільша кількість робіт, присвячених поняттям правового моделювання хронологічно належить до 1980-х років. Такий інтерес значною мірою було обумовлено інформатизацією науки. Але дослідження виявилися досить рудиментарними, в тому числі і метод моделювання, та перестали бути предметом широкої розробки вченими. Дослідженнями питань соціально-правового моделювання, моделювання загроз інформаційній безпеці присвячено праці як фахівців у сфері права, так і вчених технічних наук, таких як: А. Б. Качинський, В. М. Фурашев, О. В. Гладківська, О. Ю. Бусол, Д. В. Ланде, Т. Дж. Смедінгоф, К. Вібхут, Дж. МакЛін, Д. Деннінг та інші.

Основою більшості досліджень є принцип підходу до соціально-правового моделювання як комплексного методу у правовій інформатиці. Тобто для вирішення конкретної задачі моделюються з інформаційних позицій елементи суспільних відносин, системи обігу інформації, механізм правового регулювання, правотворчості тощо, розробляється діюча модель тих чи інших правовідносин, здійснюється аналіз отриманих за допомогою моделі даних та розробляється механізм усунення відповідної загрози. Таким чином, більшість досліджень не пропонують не тільки побудови, а й загальної характеристики комплексної дієвої правової моделі інформаційної безпеки, що надала б змогу її використання для передбачення та перевірки достатньої кількості загроз інформаційній безпеці.

Метою даного обговорення є визначення етапів побудови правової моделі та характеристики комплексної моделі інформаційної безпеки.

Забезпечення стану дотримання безпеки інформації є одним із превалюючих завдань держави у процесі побудови дієвої системи забезпечення загального механізму непорушення прав та свобод громадян, державних та громадських інтересів. Відповідно до положень Указу Президента України „Про Доктрину інформаційної безпеки України” від 08 липня 2009 року 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].

Відповідно до статті 13 Закону України „Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" від 09 січня 2007 року інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний уплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [2]. Можна погодитися з В. Петриком, який запропонував визначення інформаційної безпеки як стану захищеності особи, суспільства і держави, за якого досягається такій інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), коли сторонні інформаційні впливи не завдають їм суттєвої шкоди [3]. Прикладом більш стислого визначення є така дефініція: інформаційна безпека є процесом зберігання інформації у стані захищеності її доступності, цілісності і конфіденційності [4].

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 і здатність до перебудови та зміни власних структурних елементів.

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 упровадження дієвого механізму запобігання.

Загальний схематичний поділ джерел загроз має такий вигляд:

Рівень інформаційного імунітету – кількісно-якісна характеристика об'єкта інформаційної безпеки. Це такий стан об'єктів інформаційної безпеки, що характеризує їх здатність знижувати власну вразливість. Тобто чим вищий інформаційний імунітет, тим менше обставин, обумовлених недоліками побудови процесу функціонування об'єктів та організаційно-технічної і правової системи захисту (вразливостей).

Уразливості можуть бути класифіковані та мають таку структуру.

Об'єктивні – залежать від особливостей і технічних характеристик обладнання та устаткування обігу інформації. Такі вразливості можуть бути усунені за допомогою технічних та техніко-інженерних методів.

Суб'єктивні – мають антропогенне походження і залежать від рівня знань, досвіду та інших персональних характеристик і

властивостей суб'єктів процесу дотримання стану інформаційної безпеки. Такі вразливості можуть бути усунені організаційно-управлінськими, дисциплінарними методами.

Стихійні (абсолютні) – вразливості, породжені непередбачуваними обставинами та непрогнозованими технічними збоями, зовнішніми пошкодженнями.

Загрози – потенційно можлива подія, процес, явище або діяльність, що за допомогою низки власних особливостей має можливість уплинути на інформацію, тим самим порушивши один або кілька станів її захищеності (конфіденційність, цілісність, доступність), і, як результат, призвести до негативних наслідків порушення інформаційної безпеки.

Можливі наслідки – кількісно-якісна характеристика кінцевого стану інформаційної безпеки. Це потенційний результат упливу загрози на об'єкт, що залежить від інтенсивності загрози та рівня і стану інформаційного імунітету.

Крім того, побудова моделі інформаційної безпеки передбачає не тільки виявлення загроз та їх аналіз з метою прогнозування наслідків та оцінки можливих збитків у разі їх реалізації, а 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 важливий і той факт, що інформація є не тільки абстрактною філософської категорією, а 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 упровадження нових інформаційних технологій підвищити результативність діяльності щодо її реалізації.

Отже, на підставі вищевикладеного можна надати визначення правової моделі інформаційної безпеки – кількісно-якісний опис можливого варіанта забезпечення системи безпеки з обов'язковими 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 і фрагментарність законодавчої та нормативної бази створюють всі умови для неможливості застосування комплексного підходу до забезпечення інформаційної безпеки.

Аналіз результатів роботи з комплексною правовою моделлю інформаційної безпеки є достатнім обґрунтуванням розробки низки нормативно-правових та нормативних актів для врегулювання суспільних відносин у сфері інформаційної безпеки і побудови чіткої організаційно-сприятливої системи відповідних 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 руйнівним наслідкам.

Список використаних джерел:

1. Про Доктрину інформаційної безпеки України : Указ Президента України від 08 липня 2009 року № 514 / 2009. Офіційний вісник Президента України. – 2009. – № 20. – 677 с.

2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09 січня 2007 року № 537-V. Відомості Верховної Ради України (ВВР). – 2007. – № 12. – Ст. 102.

3. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. – Режим доступу : www.justinian.com.ua/article.php?id=3222.

4. Demopoluos associated What is Information Security? – Режим доступу : www.demop. com/articles/information-security.html.

Лихоліт Д.В.
студентка,
Національний університет «Одеська юридична академія»

ПОДАТКОВА СИСТЕМА УКРАЇНИ ТА НАПРЯМКИ ЇЇ ВДОСКОНАЛЕННЯ

В результаті переходу української економіки на європейський рівень та становлення в державі ринкових відносин, побудова досконалої та ефективної податкової системи залишається актуальною. Слід сказати,що на даний час окремі елементи податкового механізму вимагають заміни, так як діюча податкова система не відповідає в повному обсязі вимогам нинішнього стану економіки. Саме податкова система є головним джерелом формування дохідної частини бюджету України.

Податкова система є основою фінансової системи, відповідає економічному устрою країни, регулюванню економічних процесів,а також рівню розвитку продуктивних сил.