УДК 340:004

ЮДКОВА К.В., викладач кафедри інформаційного права та права інтелектуальної власності Національного технічного університету України “Київський політехнічний інститут”, юрисконсульт Національного технічного університету України “Київський політехнічний інститут”

ПОБУДОВА ПРАВОВОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Метод правового моделювання є комплексним методом забезпечення інформаційної безпеки. Дослідження загроз інформаційній безпеці та розробка засобів їх запобігання за допомогою правової моделі є можливістю боротьби з існуючими загрозами, недопущення виникнення нових загроз. Досліджено загальну процедуру впровадження процесу моделювання загроз інформаційній безпеці. Надано загальну характеристику правової моделі інформаційної безпеки.*

Ключові слова: *правове моделювання, інформаційна безпека, інформаційні загрози.*

Аннотация. *Метод правового моделирования является комплексным методом обеспечения информационной безопасности. Исследование угроз информационной безопасности и разработка средств их предотвращения с помощью правовой модели являются возможностью борьбы с существующими угрозами, недопущения возникновения новых угроз. Представлена общая процедура внедрения процесса моделирования угроз информационной безопасности. Разработана общая характеристика правовой модели информационной безопасности.*

Ключевые слова: *правовое моделирование, информационная безопасность, информационные угрозы.*

Summary. *The method of legal modeling is a complex method for provision of information security. The studying of information security threats and developing means to prevent them by using the legal model is the possibility of tackling the existing threats, preventing the emergence of new threats. The article introduces the basic procedure for the implementation of the modeling process of information security threats. A general characteristic of the legal model of information security was introduced.*

Keywords: *legal modeling, information security, information threats.*

Постановка проблеми. 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 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 рр. 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.

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 статті є визначення етапів побудови правової моделі та характеристики комплексної моделі інформаційної безпеки.

Виклад основного матеріалу. 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 08.07.09 р. 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 ст. 13 Закону України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” від 09.01.07 р. 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 вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [2]. Можна погодитися з кандидатом наук з державного управління В. Петриком, який запропонував визначення інформаційної безпеки як стану захищеності особи, суспільства і держави, за якого досягається такий 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 в 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.

Станом захищеності інформацій є такий її стан, коли зберігаються три основні її характеристики [5]:

- конфіденційність – стан інформації, за якого доступ до неї здійснюють тільки суб’єкти, що мають на неї право;
- цілісність – уникнення несанкціонованої модифікації інформації;
- доступність – уникнення тимчасового або постійного приховування інформації від користувачів, що отримали права доступу.

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 інформаційній безпеці. Таким чином моделювання доцільно проводити, визначивши:

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

Джерела загроз інформаційній безпеці класифікуються за великою кількістю критеріїв, наприклад: відповідно від носіїв загроз, за місцем виникнення, за сферою знаходження об’єкта загрози тощо. В розділі “Реальні та потенційні загрози інформаційній безпеці України” Указу Президента України “Про Доктрину інформаційної безпеки України” від 08.07.09 р. зазначено такі сфери загроз інформаційній безпеці України: зовнішньополітична, державної безпеки, воєнна, внутрішньополітична, економічна, соціальна та гуманітарна, науково-технологічна, екологічна [1].

Загальний схематичний поділ джерел загроз має такий вигляд:

Залежать від дій людини	**Залежать від технічних процесів**	**Залежать від не прогнозованих обставин**
Дії суб’єктів правовідносин, направлені на порушення інформаційної безпеки: умисні чи необережні делікти, злочини. Піддаються достатньо точному прогнозуванню.	Є наслідками тих чи інших властивостей використовуваної техніки. Менш прогнозовані.	Всі наслідки стихійних негативних явищ, непереборної сили. Неможливо прогнозувати, виникають стихійно, через це потребують впровадження постійних заходів їх усунення.

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).

Вразливості 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 вплинути 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 впливу загрози на об’єкт, що залежить від інтенсивності загрози та рівня і стану інформаційного імунітету.

Таким чином, сукупний комплексний процес моделювання загроз інформаційної безпеки включає загальні етапи:

- визначення виду кожного досліджуваного об’єкта (загрози) з формально-правового боку тлумачення. Аналіз існуючих наукових досліджень об’єкта, їх систематизація. Аналіз та узагальнення національного та міжнародного законодавства щодо зазначеного об’єкта. Результатом етапу є побудова моделі;

- використання моделі для прогнозування можливих загроз інформаційній безпеці. Результатом етапу є побудова системи можливих загроз.

- розробка методів запобігання виявленим загрозам на підставі отриманих результатів;

- аналіз результатів та встановлення того, чи узгоджуються результати спостережень із практичним застосуванням моделі і з якою точністю;

- аналіз моделі з урахуванням виявленої інформації; вдосконалення моделі;

- розробка відповідних нормативних актів для правового забезпечення інформаційної безпеки.

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 впровадження нових інформаційних технологій підвищити результативність діяльності щодо її реалізації.

Висновки.

На підставі вищенаведеного 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 організаційносприятливої 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.

Використана література

1. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник Президента України. – 2009. – № 20. – С. 18. – Ст. 677.

2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 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

5. Техническая защита информации : приказ Федерального агентства по техническому регулированию и метрологии от 29.12.05 г. № 479-ст. – Режим доступу : //www.zakon.law7.ru/ base09/part0/d09ru0812.htm

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~