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”

РІВЕНЬ ІНФОРМАЦІЙНОГО ІМУНІТЕТУ ЯК СКЛАДОВА ЧАСТИНА ПРАВОВОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *У роботі досліджено етапи характеристики об’єкта для визначення рівня його інформаційного імунітету.*

Ключові слова: *інформаційний імунітет, вразливість. інформаційні загрози, інформаційна безпека.*

Аннотация. *В работе исследованы этапы характеристики объекта для определения уровня его информационного иммунитета.*

Ключевые слова: *информационный иммунитет, уязвимость, информационные угрозы, информационная безопасность.*

Summary. *The stages of object description for the decision of its informative immunity level are explored in work.*

Keywords: *information immunity, vulnerabilities, information threats, information security.*

Постановка проблеми. Процес правового моделювання інформаційної безпеки є складним, ступеневим структурним процесом, реалізація якого здійснюється за декількома стадіями. Однією із обов’язкових стадій побудови правової моделі – є визначення рівня інформаційного імунітету об’єкта інформаційної безпеки.

Без глибокого аналізу недоліків власне самої інформаційної системи, а також всіх факторів, що впливають на її здатність до самозахисту від загроз, неможливо надати адекватну характеристику ризикам, а також визначити, які саме джерела загроз існують для тих чи інших систем.

Крім того, відсутність єдиної нормативної методичної бази правового регулювання алгоритмів дослідження об’єкта інформаційної безпеки задля визначення рівня його інформаційного імунітету значною мірою ускладнює весь процес побудови дієвої правової моделі інформаційної безпеки.

Найбільший пласт робіт, присвячених етапам моделювання інформаційної безпеки, складають роботи фахівців технічних наук, таких як С. Вихорев, С. Симонов, А. Астахов. Необхідно звернути увагу на той факт, що дане питання не є розробленим вітчизняними фахівцями з інформаційного права. Таким чином дослідження щодо етапів правого моделювання, зокрема, в сфері інформаційної безпеки, є рудиментарними та недостатніми.

Метою статті є опис такого етапу правового моделювання інформаційної безпеки, як рівень інформаційного імунітету, а також визначення основних етапів досліджень об’єкта інформаційної безпеки з точки зору його зовнішніх та внутрішніх недоліків.

Виклад основного матеріалу. Кожна із стадій побудови правової моделі інформаційної безпеки обов’язково передбачає досконале глибоке вивчення низки факторів, що впливають на об’єктивність наявних фактів, якими необхідно оперувати.

Для того, щоб виявити, чи потенційні наслідки інформаційних загроз є негативними або такі, що несуть нейтральний характер, необхідно ідентифікувати та дослідити факти та відомості щодо об’єкта загроз. Це передбачає необхідність отримання відповіді на питання, які стосуються таких аспектів, як:

– сутність загрози;

– джерело загроз;

– рівень інформаційного імунітету об’єкта загрози;

– можливі наслідки.

Перш ніж аналізувати, який саме характер будуть мати наслідки для об’єкта інформаційної безпеки, необхідно точно знати, чи здатен такий об’єкт здійснювати самостійний захист від потенційних загроз, а якщо здатний, то на якому рівні та в якій мірі будується його власна система захисту.

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) [1].

На рівень інформаційного імунітету впливає низка обставин: як внутрішні і зовнішні характеристики-недоліки або т. з. вразливості об’єкта інформаційної безпеки, так і безпосередньо властивості самого об’єкта інформаційної безпеки.

За визначенням С.В. Симонова, вразливість (англ. vulnerability) – слабкість в системі захисту, яка робить можливою реалізацію загрози [2].

Загрози інформаційній безпеці, навіть об’єктивні, не можуть виникати без достатніх на це причин, тобто безпідставно. Фактори із уражуючими ознаками так і залишаться потенційними підставами порушення інформаційної безпеки і не перетворяться на загрози в тому разі, якщо об’єкт інформаційної безпеки буде мати абсолютну можливість до самозахисту. На жаль, на сьогодні забезпечити абсолютну стійкість об’єктів інформаційної безпеки об’єктивно неможливо, таким чином, необхідно досліджувати всі можливі недоліки таких об’єктів.

Вразливості притаманні об’єкту інформаційної безпеки, невіддільні від нього і обумовлюються недоліками процесу функціонування, організаційно-технічної і правової системи захисту, умовами експлуатації та використання.

Джерела загроз можуть використовувати вразливості для порушення безпеки інформації, отримання незаконної вигоди (нанесення шкоди власнику, володільцю, користувачеві інформації). Крім того, можливе існування незловмисних дій джерел загроз щодо активізації тих чи інших вразливостей, що завдають шкоди.

Кожному типу загроз можуть відповідати ті чи інші вразливості, що активізують загрози. Усунення або істотне ослаблення вразливостей впливає на можливість реалізації загроз безпеці інформації.

Вразливості можна розділити на три групи:

– об’єктивні;

– суб’єктивні;

– випадкові.

Об’єктивні вразливості найчастіше залежать від особливостей побудови і техніко-організаційних характеристик об’єкта інформаційної безпеки, характеристик обладнання захисту, що може застосовуватися для забезпечення безпеки такого об’єкту. Повне усунення цих вразливостей неможливо, але вони можуть істотно послаблюватися інженерно-технічними методами превентивної боротьби із інформаційними загрозами.

Суб’єктивні вразливості найчастіше мають антропогенне походження. Усунення таких вразливостей досягається організаційно-правовими методами. Зокрема, одним із способів досягнення анулювання вмісту антропогенних властивостей об’єкта інформаційної безпеки є обмеження доступу до інформації, що зберігається, обробляється,передається або використовується в будь-який інший спосіб.

Незважаючи на дієвість методу обмеження інформації, необхідно звернути безпосередню увагу на той факт, що не вся інформація може мати режим обмеженого доступу, зокрема, відповідно до ст. 21 Закону України “Про інформацію”, інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація [3]. Таким чином, законодавець виділяє види інформації, що підлягає обмеженню.

Також, відповідно до положень Програми інформатизації споживчої кооперації України на 2011 – 2015 роки, інформацією з обмеженим доступом визнається інформація, що становить комерційну таємницю або є конфіденційною, споживчих товариств, споживспілок, їх підприємств (об’єднань), інших суб’єктів господарювання системи Центральної спілки споживчих товариств країни [4].

Крім того, можна навести наступне визначення інформації з обмеженим доступом, що надається у відповідності до ст. 1 Угоди між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом, так, інформація з обмеженим доступом – це інформація та матеріали незалежно від їх форми, природи та способу передачі, яким встановлені певні ступені обмеження доступу та надані відповідні грифи обмеження доступу, і які в інтересах національної безпеки та згідно з національним законодавством Сторін підлягають охороні від несанкціонованого доступу [5].

Таким чином, режим обмеженого доступу розповсюджується на інформацію, виражену в будь-якій формі та в будь-який спосіб розголошення якої може завдати шкоди приватним, комерційним, корпоративним або національним інтересам відповідних суб’єктів.

Випадкові вразливості залежать від особливостей середовища, в якому функціонує об’єкт інформаційної безпеки, а також від непередбачуваних обставин. Ці фактори, як правило, мало передбачувані і їх усунення можливо тільки при проведенні комплексу організаційно-правових та інженерно-технічних заходів з протидії загрозам інформаційної безпеки.

Крім того, всі вразливості мають різний рівень небезпеки. Відповідно, за рівнем небезпеки буде доцільним поділити вразливості на:

- критичні;
- середнього ступеня небезпеки;
- такі, якими можливо знехтувати.

Критичними вразливостями об’єкта інформаційної безпеки є такі вразливості, наявність яких знижує здатність об’єкта до самозахисту до такого рівня, коли потенційна загроза при виникненні створює небезпеку настання негативних наслідків із відсутністю можливості їх запобігти або така можливість потребує значних затрат організаційних, технічних та людських ресурсів.

Вразливостями середнього ступеня небезпеки можна вважати такі недоліки об’єкта інформаційної безпеки, наявність яких знижує здатність об’єкта до самозахисту до такого рівня, коли потенційна загроза при виникненні створює небезпеку настання негативних наслідків із ускладненням можливості їх запобігти.

Вразливостями, якими можливо знехтувати, можна вважати такі недоліки об’єкта інформаційної безпеки, наявність яких майже не зачіпає здатність об’єкта до самозахисту

або знижує його здатність до самозахисту до такого рівня, коли потенційна загроза при виникненні створює небезпеку настання негативних наслідків, але існує реальна можливість їх запобігання.

Розподіл вразливостей на відповідні рівні доцільно проводити після їх порівняння за низкою ознак. Так, до названих ознак деякі фахівці відносять наступні [6]:

– фатальність;
– доступність;
– кількість.

Під фатальністю слід розуміти ступінь впливу загрози на можливість знешкодження негативних наслідків при реалізації загрози.

Доступність характеризує рівень можливості використання вразливості джерелом загрози.

Кількість визначає, скільком елементам об’єкту інформаційної безпеки притаманні ті чи інші вразливості.

Таким чином, визначення рівня вразливостей об’єкта інформаційної безпеки є прямо необхідним для подальшого визначення всього рівня інформаційного імунітету.

Для того, щоб ідентифікувати та характеризувати недоліки об’єкта інформаційної безпеки необхідно визначити межі управління інформаційною безпекою об’єкта.

Для цього необхідно провести дослідження по наступних етапах:

1. Визначення меж об’єкта інформаційної безпеки і його оточуючого середовища.
2. Обстеження об’єкта інформаційної безпеки:

- аналіз та класифікація оброблюваної інформації, а також її поділ за категоріями доступу;

- аналіз організаційної структури об’єкта інформаційної безпеки, порядку його функціонування та/або експлуатації;

- визначення типового класу об’єкта інформаційної безпеки відповідно до чинних нормативно-правових актів України;

3. Обстеження середовища об’єкта інформаційної безпеки, включаючи:

- визначення ресурсів середовища, що використовуються для функціонування та або/ експлуатації об’єкта інформаційної безпеки;

- аналіз залежності безпеки об’єкта інформаційної безпеки від середовища його функціонування та/або експлуатації.

В процесі дослідження по вказаних етапах необхідно отримати наступні дані та відомості.

1. Перелік всіх відомостей, що є інформацією, яка потребує захисту. Крім цього, слід виокремити зі всього масиву отриманої інформації перелік відомостей, що становлять інформацію з обмеженим доступом, тобто конфіденційну, таємну або службова інформацію.

2. Характеристика всіх систем організаційного та технічного захисту об’єкта інформаційної безпеки, які є в наявності. Наприклад, розміщення засобів обчислювальної техніки і підтримуючої інфраструктури, план розташування адміністративних будівель, виробничих і допоміжних приміщень.

Додатково необхідно визначити всю структуру і склад автоматизованої системи, приміщення, в яких є технічні засоби обробки критичної інформації з урахуванням їх розташування.

3. Перелік і характеристика використовуваних автоматизованих робочих місць, серверів, носіїв інформації, в разі їх наявності.

Крім того, даний етап вимагає визначення опису інформаційних потоків, технологій обробки інформації та вирішувані завдання, порядок зберігання інформації.

Однією із важливих задач названого етапу є визначання використовуваних засобів зв’язку. Знання елементів системи засобів зв’язку дає можливість виділити критичні ресурси і визначити ступінь деталізації обстеження. Інвентаризація інформаційних ресурсів повинна провадитися виходячи з наступного аналізу їх уразливості.

4. Підведення підсумків та зведення всіх отриманих відомостей до таблиці наступного типу:

Характеристика об’єкта інформаційної безпеки			
1.1	Інформація загального доступу		
1.2	Інформація з обмеженим доступом	Конфіденційна	
		Службова	
		Таємна	
2.1	Системи захисту	Засоби обчислювальної техніки	
		Засоби підтримуючої інфраструктури	
		План розташування відповідних будівель/технічних засобів	
		Інші системи захисту	
3.1	Характеристика автоматизованих робочих місць		
3.2	Сервери, носії інформації		
3.3	Характеристика інформаційних потоків		
3.4	Характеристика вирішуваних завдань		
4.1	Зберігання інформації	Рівень доступу	
		Організаційно-правові заходи захисту	
		Технічні заходи захисту	
		Інші заходи захисту	

У результаті необхідно звести всі відомості до єдиного документу, в якому зафіксовано межі об’єкта інформаційної безпеки, перераховано ресурси та надана їх характеристика, визначена інформація, що підлягає захисту.

Отримана інформація є достатньою підставою для проведення відповідних досліджень щодо ідентифікації та класифікації вразливостей.

Таким чином, тільки після отримання та дослідження всіх вищезазначених відомостей по вказаних етапах, стає можливим перехід до сукупного визначення та

оцінки рівня інформаційного імунітету. Крім того, тільки така послідовність обробки інформації щодо об’єкта інформаційної безпеки надає можливість врахувати всі характеристики інформаційного імунітету об’єкта, а також надає більш повну інформацію на інших етапах моделювання, зокрема на етапі характеристики джерел загроз.

Висновки.

На підставі вищевідзначеного, вважаємо за доцільне розроблення відповідного нормативно-правового акту загальнодержавного значення, який містив би основні методичні матеріали, а також – впровадження інструкції із викладенням основних етапів дослідження рівня інформаційного імунітету, що слугувало б приведенню у відповідність до вимог чинного законодавства України існуючих способів та систем захисту об’єктів інформаційної безпеки.

Використана література

1. Юдкова К.В. Побудова правової моделі інформаційної безпеки // Інформація і право. – № 1(10)/2014. – С. 68-72.

2. Симонов С.В. Анализ рисков, управление рисками / С.В. Симонов // Jet Infa. – 1999. – № 1. – С. 65.

3. Про інформацію : Закон України від 02.10.92 р. № 2657-XII // Відомості Верховної Ради України (ВВР). – 1992. – № 48. – Ст. 650.

4. Про Програму інформатизації споживчої кооперації України на 2011 – 2015 роки : Постанова Ради центральної спілки споживчих товариств України від 10.11.10 р. – Режим доступу : //www.zakon.nau.ua/doc/?code=n0014626-10

5. Про взаємну охорону інформації з обмеженим доступом : Угода між Кабінетом Міністрів України та Урядом Литовської Республіки від 05.06.03 р. // Офіційний вісник України. – 2004. – № 33. – Стор. 192. – Ст. 2239.

6. Вихорев С.В. Классификация угроз информационной безопасности. – (Cnews.ru - годовой обзор). – Режим доступу : //www.masters.donntu.edu.ua/2005/fvti/vorotyntsev/library /class.pdf

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