[1] *Красноступ Г. М.* Основні напрями правового забезпечення державної інформаційної політики / Г. М. Красноступ // Бюлетень Міністерства юстиції України. – 2010. – № 10. – С. 79–85. – С. 83.

[2] *Курус І.* Цифрове телебачення – необхідність, продиктована часом / Ігор Курус : [Електронний ресурс]. – Режим доступу : http://www.nrada.gov.ua/ua/publikaciivzmi/cifrove_telebachennja___neobxidnist_prodiktovana_chasom.html

[3] План розвитку національного телерадіоінформаційного простору: затверджено Рішенням Національної ради України з питань телебачення і радіомовлення 1 грудня 2010 р. № 1684 (у редакції від 18 лютого 2015 р. № 212) // Офіційний вісник України. – 2015. – № 35. – Ст. 1042.

[4] A Digital Agenda for Europe : [Electronic resource]. – Brussels, 26.8.2010 COM(2010) 245 final/2. – Access mode: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

[5] Про телебачення і радіомовлення : Закон України від 21 грудня 1993 р. № 3759-XII (у ред. від 12 січня 2006 р.) // Відомості Верховної Ради України. – 2006. – № 18. – Ст. 155.

[6] Звіт Національної ради України з питань телебачення і радіомовлення за 2015 рік : [Електронний ресурс]. – Режим доступу : http://www.nrada.gov.ua/userfiles/file/2016/Zvitna%20informacia.pdf

Резюме

Андрусів У. Б. **Правові засади переходу України на цифрове мовлення.**

У статті аналізуються правові проблеми, пов'язані з переходом телебачення на цифровий формат мовлення. Особлива увага приділяється питанням, що виникли в ході реалізації програми впровадження в Україні цифрового телерадіомовлення. На підставі проведеного дослідження зроблено висновки, які сприятимуть заповненню існуючих прогалин та подоланню неточностей.

Ключові слова: новітні технології, цифрове телебачення, цифрове телерадіомовлення, аналогове мовлення, наземне цифрове ефірне телебачення, правова охорона.

Резюме

Андрусив У. Б. **Правовые основы перехода Украины на цифровое вещание.**

В статье анализируются правовые проблемы, связанные с переходом телевидения на цифровой формат вещания. Особое внимание уделяется вопросам, возникшим в ходе реализации программы введения в Украине цифрового телерадиовещания. На основании проведенного исследования сделаны выводы, которые будут способствовать заполнению существующих пробелов и преодолению неточностей.

Ключевые слова: новые технологии, цифровое телевидение, цифровое телерадиовещание, аналоговое вещание, наземное цифровое эфирное телевидение, правовая охрана.

Summary

Andrusiv U. **Legal basics to passing of Ukraine to the digital broadcasting.**

Legal problems, rise in the article analysed, to passing of television to the digital format of broadcasting. The special attention is spared questions, to arising up during realization of the program of introduction in Ukraine of digital TV-radio broadcast. According to the results of the analysis it is concluded that will assist filling up of existent lacunas in law and overcoming of inaccuracies.

Key words: newest technologies, Digital Television, digital TV-radio broadcast, analog broadcasting, Digital Video Broadcasting-Terrestrial, legal protection.

УДК 351.746:007

В. Д. ГАВЛОВСЬКИЙ

Владислав Данилович Гавловський, *кандидат юридичних наук, старший науковий співробітник*

ДО ПИТАННЯ ЗАХИСТУ КІБЕРПРОСТОРУ УКРАЇНИ

Величезні можливості сучасних інформаційних технологій усе більше використовуються з протиправною, зокрема злочинною метою. Вочевидь, що нині, через відсутність державних кордонів, анонімність у мережі та інші фактори кіберпростір перетворився на майже ідеальне місце вчинення злочинів.

Аналіз даних офіційної статистичної звітності за останні 14 років свідчить про тенденцію стабільного та стрімкого зростання кількості кіберзлочинів. Характерними ознаками показників кіберзлочинності є стабільне зростання частки тяжких злочинів, груповий характер їх вчинення, залежність географії поширення від фактору урбанізації.

Відповідно до єдиного звіту про кримінальні правопорушення за 11 місяців 2016 р. обліковано 815 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, з них 479 тяжких і 48 вчинені групою осіб. Порівняно з минулим роком (520 злочинів) маємо зростання на 56,7 %, а тяжких (244 злочинів) – майже вдвічі.

Значна частина кіберзлочинів вчиняється за допомогою шкідливого програмного забезпечення, поширення якого набуває все більш значущих і загрозливих масштабів.

Показовим є звіт компанії Panda Security за перший квартал 2016 р., в якому зазначається, що за три перших місяці поточного року рівень створення шкідливих програм продовжує бити всі рекорди, досягши позначки в 20 млн нових шкідливих програм, тобто в середньому – 227 тис. зразків щодня. Це більше, ніж було виявлено в першому кварталі 2015 р., коли щодня виявлялося приблизно 225 тис. зразків. Для порівняння з аналогічним періодом 2014 р. – 15 млн нових шкідливих програм і щоденна їх кількість 160 тисяч[1].

Незважаючи на величезні зусилля конкуруючих між собою фірм-виробників антивірусних засобів збитки, завдані комп'ютерними вірусами, зростають.

Одним із нових напрямів використання шкідливого програмного забезпечення з протиправною метою є програмні закладки на серверах онлайн-магазинів. Така програмна закладка перехоплює дані платіжних карток у момент їх уведення користувачем у текстове поле в браузері. У цьому випадку покупців не захищає шифрування за протоколом HTTPS, оскільки дані перехоплюються ще до шифрування.

Перші скомпрометовані сайти були виявлені в кінці 2015 року. З того часу їх кількість зросла, як мінімум, удвічі. Крім того, хакери стали використовувати все більш складні схеми для маскування. Всього в світі було виявлено 5925 онлайн-магазинів, заражених небезпечним вірусом, з яких 67 – в зоні .UA[2].

Згідно з даними компанії з комп'ютерної безпеки Endgame у 2016 р. однією з серйозних загроз для користувачів, особливо корпоративних, стало різке зростання різних видів хакерських атак з метою вимагання. Якщо за весь 2015 р. було створено близько 10 принципово нових способів, то за перший квартал 2016 р. їхня кількість вже перевищила 12.

Серед шкідливих програм, за допомогою яких проводиться вимагання, найпоширенішими є програми-шифрувальники, які блокують доступ до файлів, що зберігаються на пристроях, з подальшою вимогою викупу. Зловмисники відшукують все нові й нові вразливі місця, що дали б їм змогу проникнути на пристрій користувача.

Експерти зафіксували зростання активності кіберкампаній з використанням шкідливих WSF-файлів, вкладених в електронні листи. У червні поточного року було виявлено 22 000 подібних листів, у липні – 2 000 000, а у вересні – 2 200 000[3].

Водночас варто враховувати, що таке шкідливе програмне забезпечення було і залишається однією з найбільш поширених причин витоку та незворотної втрати важливої для фінансової, економічної, наукової та військової сфер держави інформації. Особливо небезпечними є програми-шпигуни. До того ж такі шкідливі програми постійно вдосконалюються фахівцями, які знаходять усе нові, більш витончені способи несанкціонованого проникнення до комп'ютерів користувачів та інформаційних систем.

Слід звернути увагу на те, що у нашій державі відсутній належний рівень національного антивірусного програмного забезпечення. Вочевидь, що антивірусні програмні продукти, розроблені іноземними компаніями, не можуть, з одного боку, врахувати на достатньому рівні конкретні потреби захисту національної складової інформаційного простору, що включає і закриту, таку, що належить виключно державі або охороняється нею, конфіденційну інформацію, потрапляння якої до іноземних розробників антивірусних програм є неприпустимим через фактичну шкоду навіть від цього національній безпеці України, а, з іншого, через неможливість гарантування того, що представники іноземних спецслужб не використовують антивірусні програми національних розробників для того, щоб блокувати виявлення власних програм-шпигунів. Як вбачається, і в останньому випадку використання іноземного антивірусного програмного забезпечення також є небажаним з точки зору забезпечення національної безпеки України.

Отже, єдиним прийнятним виходом у ситуації, що склалася, є розробка національного антивірусного програмного забезпечення. Так, в Указі Президента України від 1 травня 2014 р. № 449/2014 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» прямо передбачено опрацювання питань створення національного антивірусного програмного забезпечення[4].

Але, на жаль, лише через два роки у Плані заходів на 2016 рік з реалізації Стратегії кібербезпеки України, затвердженому розпорядженням Кабінету Міністрів України від 24 червня 2016 р. № 440-р, з`явився п. 18 «Організація та сприяння проведенню державної експертизи вітчизняного антивірусного програмного забезпечення», виконання якого покладено на Адміністрацію Держспецзв'язку.

Тому тематика, обрана для представленого дослідження щодо прискорення розробки національного антивірусного забезпечення, є важливою та відповідає **критерію актуальності**.

Метою даної статті є аналіз, у контексті національної безпеки України в інформаційній сфері, використання іноземних антивірусів та розробка й реалізація комплексу організаційно-практичних заходів в нашій країні щодо прискорення створення національного антивірусного програмного забезпечення, а також необхідність збереження потенціалу ІТ-фахівців.

Дослідженням проблемних питань, пов'язаних зі здійсненням організаційно-правових та організаційно-практичних заходів протидії злочинній діяльності у кіберпросторі, в контексті забезпечення національної безпеки України, займалися такі провідні вітчизняні вчені, як В. М. Бутузов, К. І. Беляков, М. В. Гуцалюк, А. І. Марущак, В. Г. Пилипчук, В. П. Шеломенцев, О. М. Юрченко, М. Я. Швець та інші. Разом із тим дослідження конкретних проблемних організаційно-практичних питань щодо протидії використанню у контексті інформаційних ресурсів нашої держави програм-шпигунів і прискорення створення національного антивірусного забезпечення досі недостатньо досліджені.

Програми-шпигуни найчастіше використовуються з метою незаконного збору розвідувальних даних спецслужбами різних держав. Останнім часом виявляються програми, які протягом кількох років незаконно

збирали різну інформацію з комп'ютерів урядових, дипломатичних, військових та наукових установ і організацій, а також окремих об'єктів критичної інфраструктури на території різних країн світу. Так, влітку 2016 р. антивірусні компанії Symantec і «Лабораторія Касперського» незалежно одна від одної виявили шкідливе програмне забезпечення Remsec, яке не могли знайти протягом п'яти років фахівці з усього світу через складність внутрішньої структури – при його розробці враховувалися всі шаблони і правила, які антивіруси використовують при пошуку шкідливого програмного забезпечення.

На початку грудня поточного року хакери зламали сайт Державної казначейської служби України й Міністерства фінансів України, а в середині місяця атакували сайт Міністерства оборони України. Фахівці стверджують, що для атаки був використаний аналог вірусу BlacEnergy, за допомогою якого рік тому було зламано системи ПАТ «Прикарпаттяобленерго». Тобто, чиновниками нічого не було зроблено, щоб запобігти новим аналогічним кібератакам, які були заздалегідь сплановані і скоординовані з єдиного центру, розміщеного у РФ.

Найбільшою у світі міжнародною приватною компанією, що працює в сфері інформаційної безпеки, є «Лабораторія Касперського». Вона веде свою діяльність в 200 країнах, 37 офісів відкрито в 32 країнах. У «Лабораторії Касперського» працює майже 3500 висококваліфікованих фахівців. Тут офіційно запевняють, що в антивірусі немає «недекларованих можливостей і «закладок», але визнали співпрацю зі спецслужбами Росії та інших держав і міжнародних організацій «у боротьбі з кіберзлочинністю», зазначаючи, що ФСБ – лише одна з таких організацій[5].

На сьогодні відповідно до Указу Президента України від 17 жовтня 2016 р. № 467/2016 «Про рішення Ради національної безпеки і оборони України від 16 вересня 2016 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» продовжено дію персональних спеціальних економічних та інших обмежувальних заходів (санкцій) щодо ЗАТ «Лабораторія Касперського» та ТОВ «Доктор Веб». Тобто, здійснювати державні закупівлі і застосовувати вищезгадане антивірусне програмне забезпечення органам влади України заборонено.

При цьому дозволяється вільно розповсюджувати це антивірусне програмне забезпечення на території України приватному бізнесу та громадянам – купувати, встановлювати й використовувати таке антивірусне програмне забезпечення. Тобто, жодних заборон або превентивних заходів на законодавчому рівні не встановлено. Також слід нагадати, що напередодні виборів в Україні зловмисниками було зламано виборчу систему ЦВК і тимчасово виведено з ладу ІТ-інфраструктуру Центрвиборчкому. При цьому встановлений на комп'ютері адміністратора ЦВК антивірус «Касперського» «чомусь» не спрацював.

Майже на 70 % комп'ютерів державних структур України встановлений антивірус NOD32, що його випускає Словацька антивірусна компанія ESET, яка допомогла терористам Донбасу, провівши аудит і опублікувавши звіт про кібершпигунство з боку українських спецслужб за владою так званих «Донецької і Луганської Народних Республік». Зазначимо, що це була ініціатива не російського дистриб'ютора, а центрального офісу антивірусної компанії в Братиславі. Російський фахівець Антон Черепанов, який давно працює в штабквартирі ESET, не просто провів і описав дослідження, а й виступив із доповіддю на цю тему на форумі Positive Hack Days, який проходив 17–18 травня в Москві.

При цьому представники антивірусної компанії ESET підтримують стосунки з представниками терористів т.зв. «ДНР» та «ЛНР», які надали конкретні теми листів і документи, на основі яких було проведено зазначене дослідження. Антивірусна компанія ESET, розкривши роботу українських хакерів, допомогла терористам, стала на бік терористів у рамках гібридної війни РФ проти України. У цьому випадку компанія перешкоджала інтересам України, що є реальною загрозою національній безпеці. Також компанія становить потенційну загрозу національній безпеці України, оскільки має доступ до комп'ютерів державних органів – антивірус NOD32 встановлено в понад 70 % державних установ, у тому числі міністерствах, які нещодавно були атаковані.

Тому, на думку фахівців, є підстави включити антивірусну компанію ESET до санкційного списку[6].

Отже, виходячи із викладеного, Україні конче необхідно мати своє потужне національне антивірусне програмне забезпечення. Тим більше, що існує певний досвід розробки таких програм. Першу вітчизняну антивірусну комп'ютерну програму (УНА/UNA) було створено на початку століття. У 2005 р. фахівці зазначали, що її український варіант за своїми технічними можливостями перевершував відомі закордонні аналоги. Проте у квітні 2007 р. підтримку і фінансування цього продукту було призупинено.

Наступною спробою забезпечити державу власним програмним антивірусним захистом було створення в 2009 р. фахівцями з ІТ-безпеки антивірусу Zillya. На сьогодні ця розробка здатна забезпечити певний рівень захисту ПК від уже відомих загроз. Для створення більш потужного антивірусного програмного забезпечення потрібна державна підтримка.

Разом із тим фахівцями у галузі ІТ-безпеки пропонуються також інші напрями створення антивірусного продукту. Серед інших – звернутися за допомогою до зарубіжних країн, які мають потужне антивірусне програмне забезпечення, наприклад, до Уряду Федеративної Республіки Німеччини, де функціонує антивірусна компанія Avira з 30-річним досвідом роботи у сфері забезпечення інформаційної безпеки, боротьби з комп'ютерними вірусами. В її програмному забезпеченні використано один із кращих алгоритмів для виявлення зараження вірусами.

За таких умов необхідно заручитися підтримкою німецького уряду для створення, як варіант, спільної компанії з розробки системи захисту і звичайно комплексу антивірусів на основі ядра AVIRA, використовуючи вміння і можливості наших науковців і програмістів та водночас –досвід і реалізовані алгоритми німецьких фахівців.

Варто зазначити, що антивірусне програмне забезпечення є дієвим засобом захисту комп'ютерів від вірусів. Хоча близько 15 % вірусів проникають у комп'ютери, незважаючи на встановлений антивірусний захист. Проте лише одних антивірусних програм для забезпечення всебічного захисту інфраструктури України недостатньо. Серед інших факторів, які впливають на забезпечення інформаційної безпеку держави, є формування достатнього потенціалу фахівців у цій сфері. До речі, жоден навчальний заклад не випускає готових вірусних аналітиків.

У листопаді 2016 р. портал DOU оприлюднив дослідження кадрового ринку IT-галузі в Україні. У поточному році в галузі працює 99,94 тис. фахівців: розробників, тестувальників, продакт-менеджерів та інших.

17,6 % опитаних працюють у компаніях «від 1 тис. співробітників». За даними рейтингу найбільших IT-компаній України, до категорії «від 1 тис. співробітників» потрапили одразу сім компаній (EPAM, SoftServe, Luxoft, GlobalLogic, Ciklum, NIX Solutions Ltd. та Infopulse), в яких загалом працюють 17,59 тис. фахівців.

Майже половина всіх зайнятих у IT-галузі живуть і працюють у Києві. Далі в рейтингу міст йдуть Харків, Львів, Дніпро, Одеса[7].

Крім цього, вищими навчальними закладами України щорічно готується близько 15 тис. фахівців цього профілю. У той же час економічна криза, турбулентна ситуація на сході України, нестабільність законодавчого поля, тиск силових структур на галузь, мляве впровадження обіцяних реформ, корупція, а також відсутність державного замовлення на таку кількість спеціалістів та їх низька заробітна платня в державному секторі призвели до загострення проблеми відтоку висококваліфікованих фахівців у сфері інформаційних технологій як за кордон, так і в «тіньовий» сектор національної економіки чи аутосорсингові компанії.

Упродовж останніх двох років Україну залишили майже 9 тис. IT-професіоналів. На тлі загального числа зайнятих ця цифра може здаватися незначною. Однак варто врахувати, що йдеться про фахівців з великим досвідом роботи чи талановитої молоді, тому відтік такої кількості професіоналів є фактором, що стримує зростання індустрії[8].

Зниження офіційного попиту на дипломованих IT-фахівців в Україні призвело до збільшення їх кількості на обліку в центрах зайнятості, через які працевлаштовується, як правило, лише кожний третій. Водночас попит на таких фахівців у світі зростає. Це викликало збільшення випадків їх працевлаштування в іноземних компаніях, де наші фахівці вважаються достатньо кваліфікованою і відносно дешевою робочою силою. Так, лише з числа випускників факультету комп'ютерних наук та кібернетики Київського національного університету імені Тараса Шевченка щороку виїжджає за кордон на роботу за спеціальністю близько 20 % найбільш підготовлених і обдарованих молодих фахівців.

Слід також мати на увазі, що великі транснаціональні компанії, такі як Microsoft, Google, Facebook, також «полюють» на українських комп'ютерних геніїв. Для цього ними організовуються різні чемпіонати світу з програмування, після яких пропонується працевлаштування. Як приклад, у минулому році 15 студентів факультету кібернетики, пройшовши конкурсний відбір, в якому брали участь студенти з усього світу, отримали можливість пройти стажування в компанії Facebook. Зазначимо, що конкурс становив 150 кандидатів на одне місце.

Випускники, які здобули кваліфікацію програміста, успішно працюють у провідних IT-компаніях, таких як: Google, Microsoft, Samsung Electonics, Luxoft, EPAM Systems, Ciklum, Globallogic, Materialise, Cargowise, Grammarly, 1C Україна, ABBYY, Railsware, d-Studio, SMK та багатьох інших.

Серед шляхів вирішення зазначених проблем є посилення державної підтримки розвитку індустрії програмної продукції, зокрема, через створення технополісів, як одного з елементів інноваційної інфраструктури. Їх розвиток у всьому світі свідчить про ефективність втіленого у них підходу до забезпечення перетворення нових ідей на унікальну науково-технічну продукцію завдяки поєднанню на певній території всіх елементів національної інноваційної системи. Технопарки сприяють навчальним і науковим організаціям у впровадженні новітніх технологій в економіку, створенні нових видів виробництв і нових робочих місць. Сьогодні програми будівництва технополісів реалізуються в Китаї, Таїланді, Індонезії, Філіппінах, Малайзії. На технічні мегаполіси перетворюються Японія та Австралія. До останнього часу така робота в Україні майже не проводиться.

У липні 2016 р. Президент України Петро Порошенко зустрівся з лідерами успішних українських стартапів з метою обговорення перспектив розвитку ринку інформаційних технологій та інновацій, взаємодії IT-сектору та держави. Глава держави позитивно відзначив розвиток стартапів в Україні, додавши, що нині 3 % українського ВВП створює саме IT-галузь. У свою чергу, представники українських стартапів звернулися до Президента України з ініціативою створення спеціального державного інституту, який буде опікуватися питаннями інновацій у IT-індустрію.

З вищевикладеного можна зробити наступні висновки та пропозиції:

1. Проблема протидії розповсюдженню та використанню інформаційних ресурсів нашої держави шкідливого програмного забезпечення є на сьогодні надзвичайно важливою для забезпечення інформаційної безпеки України та потребує підвищеної уваги з боку державних органів, що діють у цій сфері.

2. Доцільним є запровадження ініціатив держави щодо прискорення розробки національного антивірусного програмного забезпечення, особливо в умовах агресивної зовнішньої політики РФ, у тому числі й у кіберпросторі.

3. На законодавчому рівні заборонити розповсюдження в Україні антивірусного програмного забезпечення, виробником якого є компанія країни-агресора РФ – «Лабораторія Касперського».

4. Кабінету Міністрів України вивчити питання щодо створення спільної IT-компанії з розробки системи захисту і, зокрема, антивірусів на основі ядра німецької антивірусної компанії AVIRA.

5. Терміново на державному рівні потрібно вжити заходів щодо зменшення відтоку висококваліфікованих і молодих обдарованих ІТ-фахівців за кордон.

---

[1] В I квартале 2016 года ежедневно идентифицировались 227 000 образцов вредоносных программ : [Електронний ресурс]. – Режим доступа : https://habrahabr.ru/company/panda/blog/283000/

[2] Около 70 украинских онлайн-магазинов передавали данные платежных карт мошенникам : [Електронний ресурс]. – Режим доступа : http://biz.nv.ua/economics/okolo-70-ukrainskih-onlajn-magazinov-peredavali-dannye-platezhnyh-kart-moshennikam-246466.html

[3] Киберпреступники разработали новую технику распространения вредоносных программ : [Електронний ресурс]. – Режим доступа : https://securenews.ru/wsf-files/

[4] Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» : Указ Президента України від 1 травня 2014 р. № 449/2014 : [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/449/2014

[5] Антивірус Касперського: «ворог» вже всередині : [Електронний ресурс]. – Режим доступу : http://tsn.ua/blogi/themes/o_voine/antivirus-kasperskogo-vorog-vzhe-vseredini-351830.html; Уряд заборонив користуватися програмами «Лабораторії Касперського»! : [Електронний ресурс]. – Режим доступу : http://narodna.pravda.com.ua/discussions/56056fa4aca02/

[6] Як словацька антивірусна компанія ESET працює на терористів Донбасу : [Електронний ресурс]. – Режим доступу : http://texty.org.ua/pg/news/textynewseditor/read/68029/Jak_slovacka_antyvirusna_kompanija_eset_pracuje_na

[7] В Україні порахували ІТ-фахівців : [Електронний ресурс]. – Режим доступу : http://studway.com.ua/porakhuvali-it-fakhivciv/

[8] Около 9 тысяч IT-специалистов покинули Украину : [Електронний ресурс]. – Режим доступа : http://hubs.ua/news/okolo-9-ty-syach-it-spetsialistov-pokinulo-ukrainu-80597.html

Резюме

Гавловський В. Д. **До питання захисту кіберпростору України.**

У статті, на підставі проведеного аналізу, наводиться аргументація щодо необхідності прискорення розробки національного антивірусного програмного забезпечення, розкриваються проблемні питання стосовно ІТ-фахівців.

Ключові слова: шкідливе програмне забезпечення, антивірус, ІТ-фахівці.

Резюме

Гавловский В. Д. **К вопросу защиты киберпространства Украины.**

В статье, на основе проведенного анализу, приводится аргументация необходимости ускорения разработки национального антивирусного программного обеспечения, раскрываются проблемные вопросы ІТ-специалистов.

Ключевые слова: вредное программное обеспечение, антивирус, ІТ-специалисты.

Summary

Havlovskyy V. **On the issue of protection of cyberspace Ukraine.**

The article, based on our analysis, the argument invoked the need to accelerate the development of domestic anti-virus software, reveals the problematic issues of IT specialists.

Key words: harmful software, antivirus software, IT-specialists.

УДК 347.772

О. А. РАССОМАХІНА

Ольга Андріївна Рассомахіна, *кандидат юридичних наук, доцент Київського університету права НАН України*

АБСОЛЮТНА ПІДСТАВА ДЛЯ ВІДМОВИ В НАДАННІ ПРАВОВОЇ ОХОРОНИ ТОРГОВЕЛЬНИМ МАРКАМ – ЇХ ОПИСОВИЙ ХАРАКТЕР

Питання про те, чи має позначення, яке заявлено на реєстрацію в якості торговельної марки, розрізняльну здатність, є складним. Для його вирішення необхідно мати спеціальні знання про саму розрізняльну здатність і про факти, які впливають на її набуття внаслідок використання або ослаблення (розмивання знака). За загальними правилами про розрізняльну здатність товарний знак не повинен складатися виключно із звичайного слова (слово не повинно бути звичайним саме стосовно об'єкта, що ним маркується), бути видовим, описовим чи необхідним позначенням. Вимога про те, що знак не повинен бути описовим позначенням, як бачимо, входить до вимог про розрізняльну здатність.

Проте, закріплення дефініції даного критерію охороноздатності українське законодавство досі оминає, а лише визначає його змістове наповнення. Пропонуємо дослідити генезис нормативного закріплення даного
