УДК 330.341

Жаворонкова Г.В.
доктор економічних наук,
професор кафедри економіки
Інституту економіки і менеджменту
Національного авіаційного університету.

Крачок Л.І.
кандидат економічних наук,
редактор журналу «Прибуткове свинарство»

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ТЕХНОЛОГІЧНОЇ БЕЗПЕКИ

INFORMATION SECURITY AS A PART OF PROCESS SAFETY

АНОТАЦІЯ

У статті досліджено теоретичні аспекти інформаційної безпеки у контексті забезпечення технологічної безпеки України. Визначено основні проблеми забезпечення інформаційної безпеки, а також ймовірні загрози для національної безпеки країни. Запропоновано основні напрями діяльності щодо забезпечення потрібного рівня інформаційної безпеки в Україні.

Ключові слова: інформаційна безпека, технологічна безпека, кіберзлочинність, інформаційні технології, загрози безпеки.

АННОТАЦИЯ

В статье исследованы теоретические аспекты информационной безопасности в контексте обеспечения технологической безопасности Украины. Определены основные проблемы обеспечения информационной безопасности, а также вероятные угрозы для национальной безопасности страны. Предложены основные направления деятельности по обеспечению необходимого уровня информационной безопасности в Украине.

Ключевые слова: информационная безопасность, технологическая безопасность, киберпреступность, информационные технологии, угрозы безопасности.

ANNOTATION

This article explores the theoretical aspects of information security in the context of the process safety of Ukraine. The basic problem of information security and potential threats to the national security of the country are defined. The basic directions of activity to ensure the necessary level of information security of Ukraine are proposed.

Keywords: information security, process safety, cybercrime, information technology, security threats.

Постановка питання. Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона має бути орієнтована не тільки на захист стратегічних суб'єктів інформаційних ресурсів, а й конституційних інтересів країни. На сьогодні інформація стала ще й потужним інструментом забезпечення конкурентних переваг. Тому від правильного її застосування і захисту безпосередньо залежать національні інтереси державної безпеки.

Аналіз останніх досліджень і публікацій. Дослідженню різних аспектів питання інформаційної безпеки України, її стану і перспектив розвитку, а також проблем забезпечення свої наукові праці присвятили такі вітчизняні науковці: І. Арістова, М. Бебінська, А. Гальчинський, М. Гуцалюк, Я. Жаліло, А. Колодюк, Є. Макаренко, Я. Малик, В. Петрик, А. Петров та інші.

Виділення невирішених раніше частини загальної проблеми. Попри наявність великої кількості досліджень та публікацій, питання інноваційної безпеки як складової забезпечення економічної безпеки недостатньо висвітлені і потребують подальшого вивчення.

Мета статті. Дослідити основні загрози гарантування інформаційної безпеки України та запропонувати можливі шляхи їх подолання.

Виклад основного матеріалу дослідження. Зміст поняття «інформаційна безпека» розкривається в практичній діяльності, наукових дослідженнях, а також в нормативно-правових документах.

Згідно із законодавством України, інформаційна безпека – це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення 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» [1].

За В. Петриком, інформаційна безпека – це стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток, за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди [2].

Інформаційна безпека діє за трьома основними принципами: конфіденційність, цілісність та доступність. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність означає захист релевантності і повноти інформації та програмного забезпечення. Доступність – це забезпечення інформацією і основними послугами користувачів в потрібний для них час і формі.

Проблеми інформаційної безпеки можна поділити на три великі групи [3]:

1) гуманітарного характеру – проблеми, що виникають в зв'язку з безконтрольним використанням і розповсюдженням персональних даних громадян, вторгненням їх в приватне життя;

2) економічного і юридичного характеру – проблеми, що виникають в результаті витоку,

викривлення і втрати комерційної інформації, крадіжок брендів та інтелектуальної власності, розкриття фінансової інформації про майновий стан громадян, промислового шпіонажу та розповсюдження матеріалів, що наносять шкоду діловій репутації;

3) політичного характеру – проблеми, що виникають через інформаційні війни, кіберзлочини та електронні розвідки у ворожих інтересах для компрометації держави, атак на інформаційні системи важливих оборонних, транспортних, фінансових та промислових об'єктів, неповного інформування та дезінформації керівників великих інституцій та підприємств.

Проблема створення наукової методології заданого рівня захищеності інформаційних ресурсів протягом усього періоду їх експлуатації є важливою і актуальною. Рішення даної проблеми пов'язане з послідовним вирішенням двох часткових завдань: по-перше, кількісного оцінювання рівня захищеності; по-друге, прийняття рішення про необхідність зміни характеристик і параметрів системи захисту інформації (СЗІ) з метою підтримки заданого рівня захищеності.

Інструментальні засоби оцінки рівня захищеності (ризики порушення інформаційної безпеки) повинні бути засновані на сучасних базах даних і знань в сфері захисту інформації, щоб дозволяти будувати структурні об'єктно-орієнтовані моделі інформаційної системи, а також моделі ризиків окремих сегментів корпоративної інформаційної системи.

Застосування методів системного аналізу до дослідження проблеми захисту інформації диктується вимогами практики, яка поставила фахівців перед необхідністю проектувати складні системи захисту інформації, вивчати процеси, управляти ними в умовах невизначеності, неповноти інформації, дефіциту часу і обмеженості ресурсів.

Таким чином, вирішення актуальної сьогодні науково-технічної проблеми управління системою захисту інформації в корпоративних інформаційних системах пов'язано з необхідністю розробки комплексу науково обґрунтованих методів і методологій в рамках створення теорії інтелектуального забезпечення інформаційної безпеки.

Багато дослідників зазначають, що інформаційна революція суттєво впливає на геополітичну карту світу та світовий інформаційний розвиток, тому потрібно розглядати її як важливий геополітичний фактор, який здатний змінити відносини між центрами сили, регіонами та державами. Дана теза висуває перед кожною державою комплекс складних інформаційних проблем міжнародного характеру:

1) мова йде про побудову системи міжнародних відносин у нових умовах інформаційної прозорості державних кордонів;

2) актуальною стає розробка державної політики по відношенню до світових відкритих комп'ютерних мереж і забезпечення входження в них національних та корпоративних інформаційних і телекомунікаційних мереж з точки зору захисту національних інтересів та інформаційної інфраструктури;

3) реальними проблемами національної і міжнародної безпеки стають можливості використання інформаційних технологій в якості інформаційної зброї, а також загроза інформаційного тероризму.

Гарантувати захист та контроль національного інформаційного простору можна лише за умови вмілого поєднання двох головних підходів: створення потужних інформаційних потоків, що підтримують життєдіяльність системи символів, настанов та стереотипів, а також забезпечують її експансію в навколишній світ; розумне обмеження доступу до інформації, контроль за інформаційними потоками.

Актуальність застосування другого підходу пояснюється не лише проблемами збереження державної таємниці та припинення підривної протиправної діяльності. Існує чимало й інших питань, вирішення яких пов'язане з безпекою інформаційного простору України. Отже, стан захисту національного інформаційного простору не повністю відповідає сучасним потребам і можливостям держави.

Гостро постає питання боротьби з комп'ютерними злочинами. Згідно з ДСТУ 2938-94 «комп'ютерний злочин – це злочин, що здійснюється через використання, модифікування або знищення даних, технічних чи програмних засобів».

Таблиця 1

Ймовірні загрози безпеці інформації в мережі Інтернет і рішення щодо її захисту

Різновид загрози	Рішення	Технологія	Дії
Дані навмисно перехоплюються, читаються і/або змінюються	Шифрування	Симетричне або несиметричне шифрування	Кодування даних, яке перешкоджає їх читанню або викривленню
Невірна ідентифікація себе користувачем з метою шахрайства	Аутентифікація	Цифровий підпис	Перевірка ідентичності відправника, одержувача і повідомлення
Несанкціонований доступ до інформаційних систем	Брандмауер	Брандмауери, приватні віртуальні мережі	Фільтрація трафіку, який йде до мережі або на сервер
Кіберсквотинг (недобросовісна реєстрація доменних імен)	Інтелектуальна власність	Правовий захист	Зареєструвати ім'я домена як торгову марку
Шахрайство з платіжними картками в інтернет-банкінгу	Мережеві гроші	Paypal – інтерфейс для пластикової картки	Старт-картка з вбудованим мікропроцесором

На конференції країн Великої вісімки щодо проблем кіберзлочинності, яка відбулася ще у жовтні 2000 р., міністр закордонних справ Німеччини Йошка Фішер відзначив, що збитки від кіберзлочинів сягають 100 млрд німецьких марок щорічно. За оцінками Рахункової палати уряду США щорічні збитки від розкрадань і шахрайств, вчинених за допомогою інформаційних технологій лише через Інтернет, сягала 5 млрд дол. США [4].

Основною проблемою безпеки електронної комерційної взаємодії в Інтернеті з моменту виникнення мережі була проблема передачі закритої інформації, а саме: номерів кредитних карток, сум платежів тощо через відкриту мережну систему. Ймовірні загрози безпеці інформації, що передається в мережі, разом з рішеннями, які дозволяють організувати і значно підвищити захищеність даних, наведено в таблиці 1.

У Великобританії набрав чинності закон, відповідно до якого в особливо серйозних випадках, коли хакер поставив під загрозу безпеку країни, намагався вплинути на політику уряду або залякати громадськість, злочин характеризується як терористичний акт і карається відповідним чином. В австралійському парламенті ще в 1999 р. було прийнято закон про регулювання змісту в Інтернеті. Закон передбачає кримінальну відповідальність провайдерів Інтернет-послуг за фізичне розміщення (хостинг) забороненої інформації або надання доступу до неї.

Комітет у справах законодавства Ради Європи рекомендує уніфікувати кримінальне законодавство з питань комп'ютерних правопорушень та передбачити відповідальність за такі злочини: незаконний доступ; нелегальне перехоплення інформації; втручання у дані; втручання у систему; зловживання пристроями; підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з авторським правом та інші.

У Міжвідомчому науково-дослідному центрі з проблем боротьби з кіберзлочинністю розроблено Концепцію реалізації державної політики щодо боротьби з кіберзлочинністю в Україні. Зазначений проект пройшов широке обговорення, в якому брали участь кримінологи, психологи, соціологи, працівники правоохоронних органів, освітніх установ, комерційних підприємств.

Із введенням Закону «Про захист інформації в автоматизованих системах» Карний кодекс був доповнений ст. 198 (1) «Порушення роботи автоматизованих систем», в якій передбачається покарання за зловмисне втручання до роботи автоматизованих мереж, що призводить до перекручення або знищення інформації, а також покарання за розповсюдження програм і технічних засобів, що призначені для незаконного проникнення до автоматизованих мереж і може призвести до перекручення та знищення інформації чи носіїв інформації.

У міру дедалі більшої комерціалізації Інтернету поширюється боротьба за доменні імена і використання торгових марок в мережі. З метою подальшого перепродажу доменного імені правовласнику ідентичного або схожого для переплутування товарного знаку чи іншого засобу індивідуалізації, широке розповсюдження в мережі одержало явище «кіберсквотинг», або його ще називають «кіберпіратство».

Сьогодні в зоні.ua кожні чотири хвилини з'являється нове доменне ім'я [5]. За оцінками експертів, щорічні обсяги даного ринку (реєстрація й підтримка чинності) становлять понад 20 млн. грн. Кіберсквотери, користуючись безконтрольністю, а також тим, що така реєстрація не потребує значних фінансових витрат, реєструють на себе значну кількість різноманітних доменних імен, виставляючи їх згодом на продаж або пропонуючи власникам відомих знаків для товарів та послуг. Процеси проти українських кіберсквотерів уже розглядає Арбітражний центр Всесвітньої організації інтелектуальної власності. Тому є очевидною необхідність ухвалення спеціального законодавства, яке б визначало статус не тільки доменних імен, але й їхніх власників, а також правове становище реєстру доменів та порядок його діяльності.

Останнім часом в мережі Інтернет активізувалися атаки на сайти та сервери державних установ та організацій у фінансово-банківській сфері. Найпоширенішим видом хакерських впливів є так звані атаки, або «відмова в обслуговуванні». Схема досить проста. Велика кількість комп'ютерів (від декількох сотень і більше), програмне забезпечення яких спеціальним чином дистанційно модифікується, за командою хакерів починає одночасно направляти масові запити на відповідний ресурс, серйозно порушуючи чи повністю блокуючи роботу. Тривалість атак може продовжуватись декілька діб. Це призводить до прямих збитків, а також завдає шкоди престижу й авторитету відповідної установи.

Серед українських компаній, які застосовують засоби захисту з інформаційної безпеки, найбільший відсоток складають представники великого та середнього бізнесу. При цьому, комплексні рішення захисту, в основному, використовують банки і великі бюджетні організації. Для перших небезпека втрати банківської інформації є завжди актуальним питанням. А державні структури користуються засобами захисту, виходячи з вимог українського законодавства. Згідно з українським законодавством, угоди, однією із сторін яких є юридичні особи, повинні укладатися тільки у письмовому вигляді. Тому довгоочікуваним став закон України «Про електронні документи та електронний документообіг», який вступив у силу з 01.01.2004 р. та надав юридичний статус подібним угодам, тобто визнав електронний підпис.

Загалом проблеми забезпечення безпеки за своєю сутністю зводяться до проблеми захисту електронного документообігу. Тому специфіка ведення електронного бізнесу вимагає, щоб в

системі забезпечення безпеки були передбачені такі можливості:

– забезпечення конфіденційності інформації в процесі її створення, зберігання, обробки та обміну;

– контроль цілісності даних під час обробки та передачі по каналах зв'язку;

– аутентифікація інформації, що включає питання справжності, авторства та часу створення;

– ідентифікація учасників інформаційного обміну;

– попередження несанкціонованого доступу до ресурсів інформаційно-обчислювальних систем, в тому числі зміни процесів їх функціонування.

Кожний з перерахованих напрямків забезпечення безпеки електронного бізнесу має свої відпрацьовані методи захисту, причому безперервний розвиток інформаційних технологій вимагає постійного вдосконалення цих методів.

На жаль, існуюча система нормативних актів, яка направлена на захист інформаційних ресурсів, на даний час недостатня і може лише частково вирішити проблеми суспільних відносин в інформаційній економіці. Досвід інших країн свідчить, що захист повинен починатись на ранньому етапі, коли реальні втрати ще не нанесені; необхідні норми, які забороняють під загрозою покарання за законом несанкціонований доступ до комп'ютера та ознайомлення з комп'ютерними даними, а також зміну чи знищення цих даних; зберігання та розробка засобів для отримання незаконного доступу також має тягнути за собою карні дії.

Втім діяльність суб'єктів інформаційних відносин у глобальній комп'ютерній мережі Інтернет теж потребує відповідного правового регулювання. Відповідні законодавчі та підзаконні нормативні акти повинні враховувати напрацювання міжнародних організацій у даній сфері та, зокрема, Європейського Союзу. Це дозволить перетворити українську складову мережі на ефективний механізм розбудови демократичного суспільства, протидії корупції та організованій злочинності.

Значні проблеми в галузі законодавчого врегулювання розвитку інформаційних систем пов'язані з їх приватизацією. Якщо спробувати накласти основні положення наявних законодавчих та підзаконних актів на реальні господарські відносини, то досить виразно простежуються значні неузгодженості та дублювання в нормативно-правових актах. Фактично інформаційний простір та його складові як об'єкти правової кваліфікації мають досліджуватись відокремлено. Ця вимога набуває особливого значення з огляду на прискорення інтернаціоналізації інформаційного простору та можливої монополізації його окремих секторів.

Подальше удосконалення правового забезпечення розвитку інформаційного простору в Україні вимагає формування узгодженої законодавчої та нормативної бази, яка чітко визначить умови комерціалізації та розповсюдження інформаційних продуктів, обґрунтує критерії їх вартісного виміру, дозволить вибудувати гнучкий механізм цивілізованої реалізації прав юридичних та фізичних осіб на інформаційні ресурси на внутрішньому і зовнішньому ринках. При цьому має враховуватись необхідність введення законодавчих обмежень на розповсюдження інформації для гарантування національних науково-технічних та економічних інтересів.

На сьогодні правові акти, які регулюють відносини в інформаційній діяльності були об'єднані в єдиний комплексний правовий блок – інформаційне право, в який крім названих законів пропонувалось внести пакети законів про патентно-ліцензійну діяльність, наукову і науково-технічну експертизу, авторське право, інтелектуальну власність, технічний захист інформації тощо. В загальному виді сукупність норм права повинна охоплювати всі відносини між суб'єктами права, що існують у сфері інформатизації, інформаційній діяльності та капіталізації суб'єктів ринку.

Таким чином, забезпечення можливості взаємного поєднання і взаємодії інформаційних продуктів та послуг стали головними задачами для України. Процес стандартизації повинен бути переглянутий із метою його прискорення і посилення щодо орієнтації на вимоги ринку. Застосування сукупності адекватних апаратних засобів та методів правового захисту на всіх рівнях ведення електронного бізнесу дозволить побудувати ефективну та надійну систему забезпечення інформаційної безпеки як складової технологічної безпеки. Така система дозволить знизити, а в багатьох випадках і попередити, можливі збитки від деструктивних впливів на компоненти та ресурси систем електронного бізнесу. Впевненість в безпеці електронного бізнесу може бути досягнута тільки в результаті скоординованих дій, що здійснюються в процесі розробки, оцінки та експлуатації об'єкта інформаційної безпеки.

Виходячи з вищевикладеного, можна виділити основні напрями забезпечення потрібного рівня інформаційної безпеки в Україні:

1. Удосконалення законодавства і контроль за його дотриманням в сфері інформаційної безпеки.

2. Збільшення комп'ютерної та інформаційної грамотності населення.

3. Державі необхідно зобов'язати підприємства створювати і впроваджувати системи інформаційної безпеки, що буде забезпечувати комплексний захист інформації і в країні в цілому.

4. Використовувати виключно ліцензійні засоби захисту інформації та послуги перевірених фірм, що мають ділову репутацію і ліцензію на діяльність.

5. Державі необхідно виділяти кошти на захист комерційних таємниць, оскільки витік

такої інформації може призвести до значних негативних наслідків, а також погіршити імідж країни та її інвестиційну привабливість.

В свою чергу, створюючи системи захисту інформаційних ресурсів, необхідно враховувати: по-перше, для ефективного захисту потрібна реалізація цілого ряду різнорідних механізмів, які можна поділити на три групи: юридичні, організаційно-економічні і технологічні; по-друге, хоча розробкою заходів захисту стосовно до кожної з трьох груп повинні займатися фахівці відповідних галузей знань, кожен з яких застосовує свої способи і методи для досягнення заданих цілей, кінцевий успіх залежатиме від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними поняттями, способами і механізмами захисту.

Висновки. Таким чином, інформаційна безпека є однією із найважливіших складових технологічної безпеки та гарантом захисту національних інтересів України. На рівні держави вона досі залишається поза увагою, що може призвести до проблем гуманітарного, економічного, юридичного та політичного характеру. Тому забезпечення інформаційної безпеки має стати головним завданням країни, а починати її варто із розробки необхідних нормативно-правових актів – інформаційного права.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Інформаційна безпека [Електронний ресурс]. – Режим доступу: ukr.vipreshebnik.ru/entsiklopedia/55-i/1943-informatsija-bezpeka.html.
2. Петрик В.М. Сутність інформаційної безпеки держави, суспільства та особи / В.М. Петрик// Юридичний журнал. – 2009. – № 5. – С. 122–134.
3. Петров А.А. Анализ системы информационной безопасности в Украине / А.А. Петров, А.А. Ухань // Безпекознавство: теорія та практика: Матер. І Всеукр. наук.-практ. інтернет-конф., 15 березня–15 квітня 2013 р., м. Луганськ. – 2013. – С. 254–256.
4. Гуцалюк М.В. Правове регулювання суспільних інформаційних відносин в Інтернеті / М.В. Гуцалюк // Науковий вісник НАВСУ, 2001. – № 5. – С. 225.
5. Технологічний імператив стратегії соціально-економічного розвитку України: [монографія] / [Л.І. Федулова, Ю.М. Бажал, В.Л. Осецький та ін.]; за ред. Л.І. Федулової; НАН України; Ін-т екон. та прогнозув. – К., 2011. – 656 с.