Во-вторых. При принятии решений не учитывается, что внедрение системы защиты – это весьма длительный и кропотливый процесс. Бытует мнение, что после выделения финансовых средств на следующий день появится система безопасности. К сожалению, это не так. И чем раньше придет понимание этого, тем раньше прекратится неэффективная трата финансовых средств.

В-третьих. Разработка и внедрение полноценной системы защиты требует наличия квалифицированных специалистов в области информационной безопасности. Сетевые администраторы не являются и никогда не будут этими специалистами. У них хватает ежедневных проблем, на которые уходят все силы и время. Надежды на разработчиков программного обеспечения тоже маловероятны. У них хватает проблем с сопровождением разработанных продуктов и постоянной их адаптацией под изменяющиеся требования заказчиков. Кроме того, системные администраторы и разработчики в свою очередь являются фактором риска и на сегодняшний день достаточно большим.

В-четвертых. К кому обратиться, если вы, наконец, решили, что вашей компании или организации необходимы консалтинговые услуги в области информационной безопасности; кого предпочесть, чтобы ваш заказ был качественно выполнен, а итогом работы был не только отчет в виде списка уязвимых мест, полученного автоматическими сканерами безопасности, наподобие SATAN?

Мы можем порекомендовать обращаться к услугам фирм, которые специализируются в области информационной безопасности и обязательно (!) имеют специальные лицензии Департамента специальных телекоммуникационных систем и защиты информации.

Кроме того, вы можете обращаться непосредственно к автору данной статьи за консультациями и помощью. Телефон (044) 534 2540, e-mail: Byuriy@bartec.kiev.ua.

Литература: 1. Computer Security Issues & Trends / 2001 CSI/FBI Computer Crime and Security Survey – Vol. V11, No. 1

УДК 681.3:34

ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ДЕРЖАВНИХ ОРГАНІВ УКРАЇНИ

Ігор Близнюк, Вячеслав Шорошев
НДІ НАВС України

Анотація: **Розглядаються основи нормативного та правового забезпечення захисту інформації в комп'ютерних системах, їх регулятивні та захисні функції, напрямки, об'єкти і суб'єкти, правовий статус, режим та рівні.**

Summary: **In the article the objects and subjects, directions, legal status, mode and levels are considered a fundamentals of normative and legal maintenance of protection of the information in computer systems, them regulations and protective functions.**

Ключові слова: **Нормативне та правове забезпечення, правовий статус, рівні правового режиму.**

Одним із завдань правового забезпечення державної політики в сфері інформатизації та формування інформаційних ресурсів є створення нормативно-правових засад, включаючи питання підготовки, введення і коригування нормативно-правових актів, які забезпечують функціонування інформації як продукту суспільного виробництва, регулюють доступ до такої інформації, визначають правила обертання інформаційних потоків у відомчій мережі та інше. Як свідчить досягнутий досвід забезпечення безпеки інформації в комп'ютерних системах [1], успішність захисту інформації в комп'ютерних системах залежить від нормативно-правового забезпечення (до 60%), апаратно-програмного забезпечення (до 30%) та організаційних заходів (до 10%). Ця пріоритетність поступово, зі зростанням правової та технічної дисципліни персоналу комп'ютерних систем та досвіду їх експлуатації, перерозподіляється до апаратно-програмного забезпечення та оперативних організаційних заходів забезпечення безпеки.

Основними **напрямками** правового забезпечення захисту інформації в комп'ютерних системах (КС) України є:

- захист інформації в інтересах її власників;
- захист інформації в інтересах держави, юридичних і фізичних осіб, що є споживачами цієї інформації;
- захист інформації в інтересах юридичних і фізичних осіб, про яких накопичується, зберігається, опрацьовується і передається ця інформація.

При цьому мають враховуватися економічні і морально-етичні аспекти володіння інформацією.

Використання комп'ютерних систем для обробки інформації залежить від двох основних **функцій** правового забезпечення:

- регулятивної, яка полягає у встановленні правового режиму розробки, створення, функціонування і взаємодії КС, їхнього правового статусу;
- захисної, яка полягає у встановленні регламенту доступу обслуговуючого та технічного персоналу до елементів КС, у розмежуванні доступу до інформації, яка оброблюється, накопичується та передається, у юридичній відповідальності власників і персоналу інформаційних систем за порушення цілісності інформації, а також у юридичній відповідальності за порушення прав власності на інформацію.

Об'єктами правового забезпечення захисту інформації в КС мають бути:

- технічні засоби зв'язку, елементи інформаційних систем та комплекси;
- документи, дані, інші матеріали, опрацьовані і передані технічними засобами КС;
- програмне забезпечення КС, що здійснює обробку і передачу даних та управління роботою відповідних технічних засобів;
- організаційні структури (підрозділи та служби), що безпосередньо займаються інформаційною діяльністю із застосуванням КС.

Суб'єктами правового забезпечення захисту інформації в КС є співробітники державних органів, які займаються інформаційно-комп'ютерною діяльністю.

Захист інтересів співробітників державних органів, громадян, зайнятих інформаційно-комп'ютерною діяльністю, здійснюється відповідно до Цивільного кодексу, Кримінального кодексу, авторського права та норм різних галузей права тощо.

Правовий захист інформації (даних, програм) ґрунтується на правових засадах забезпечення безпеки інформаційних систем, які складають: Конституція України, Закони України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про науково-технічну інформацію", Концепція (основи державної політики) національної безпеки України, Концепція технічного захисту інформації в Україні, а також законодавство про інтелектуальну власність та авторське право. При цьому мають бути враховані такі особливості, як неможливість розкрадання інформації в традиційному розумінні, необхідність урахування шкоди, що викликається втратою (копіюванням) інформації, а також те, що інформація в КС може бути спільною власністю декількох суб'єктів.

Інформація в КС повинна мати визначений **правовий статус** та має бути захищеною на всіх етапах, починаючи з моменту її створення.

Введена в КС інформація може бути предметом власності різноманітних суб'єктів і має розглядатися як об'єкт (продукт) обробки в КС із визначеним на правовій основі норм чинного законодавства статусом, встановленим користувачем (власником) відповідно до рівня обмеженості доступу.

Інформація, укладена в **конструкції** фізичних елементів КС, має розглядатися як предмет інтелектуальної власності та авторського права їх розроблювачів.

Інформація, **укладена** в КС та їх програмне забезпечення, бази і банки даних, розглядається як їх експлуатаційна частка і потребує захисту з урахуванням класу КС, рівня обмеженості введеної (опрацьованої) інформації, правового режиму самих програм і алгоритмів, правового статусу власника КС та елементів КС.

Нова інформація, як продукт обробки, що створена за конкретним технологічним циклом (процесом машинної обробки), а також в ході роботи персоналу КС, є власністю користувача, замовника або власника КС, які визначають рівень обмеженості доступу до неї.

Правові відношення між власником КС, власником інформації і юридичними та фізичними особами, які є споживачами інформації, регулюються цивільним, адміністративним, трудовим законодавствами, а у випадку настання суспільно небезпечних наслідків – відомчими наказами, а також кримінальним законодавством України.

Для повноти правового забезпечення безпеки інформації мають бути розроблені і додаткові (специфічні) **механізми** встановлення відповідальності порушників ТЗІ, які враховують поряд із навмисними діями відповідальність розроблювачів КС за їх програмне забезпечення, за можливі аварії і катастрофи, пов'язані з помилками в проектуванні, а також відповідальність адміністрації КС за невірне встановлення правил розмежування доступу (ПРД) у даній КС. Усі аспекти правового забезпечення безпеки інформації в КС України також мають відповідати нормам міжнародного права.

Правовий режим обробки інформації з використанням комп'ютерних технологій і правові умови для ефективного застосування захищеної КС ґрунтуються на наступних рівнях правового забезпечення.

Перший рівень складають закони, розроблені і прийняті Верховною Радою України та спрямовані на забезпечення безпеки інформації, визначення формування і проведення політики в цій галузі.

Другий рівень складають акти Президента України та Кабінету міністрів, що забезпечують реалізацію законодавства в галузі безпеки інформації.

Третій рівень складають різноманітні норми, стандарти і класифікатори в галузі безпеки інформації в КС.

Четвертий рівень включає комплект локальних норм, положень, інструкцій, методичних рекомендацій з комплексного захисту інформації в КС державних органів України.

Окрему групу складають міжнародні акти.

Нормативне забезпечення. Поряд з викладеним необхідно звернути увагу на те, що в умовах насичення усіх сфер суспільства засобами обчислювальної техніки і утворюваними на їх базі КС, безпека інформації забезпечується в основному дотриманням вимог і положень відомчих нормативно-методичних документів. Різноманітність цих документів, неузгодженість між собою окремих положень, що в них міститься, не дозволяє в повному обсязі реалізувати єдину політику в цій галузі, а отже може призводити до невиправданих інтелектуальних і економічних втрат. Тому створення на правових основах єдиної державної системи нормативного забезпечення в галузі безпеки інформації в КС є найважливішим завданням. До складу системи нормативного забезпечення має включатись і нормативно-технічне забезпечення.

Основними завданнями системи нормативного забезпечення захисту інформації КС в Україні є:

- створення й упорядкування внутрішньовідомчих стандартів ТЗІ, нормативних документів ТЗІ на базі існуючого фонду державних стандартів у цій галузі, особливо щодо ліцензування та сертифікації як окремих елементів КС, так і КС в цілому;
- розробка нормативних документів, що регулюють правовий статус інформації та її обіг в державних органах України;
- запобігання дублюванню робіт із стандартизації КС і систем захисту, що призводить до неоднозначності тлумачення термінів та визначень з питань ТЗІ;
- скорочення обсягів фондів галузевих стандартів у галузі захисту інформації в КС;
- уніфікація вимог, запропонованих до КС у захищеному виконанні;
- забезпечення сумісності і взаємодії КС у захищеному виконанні різного рівня і призначення;
- підвищення якості КС у захищеному виконанні при одночасному зниженні трудовитрат;
- підвищення ефективності функціонування захищених КС.

Нормативне забезпечення щодо систем захисту інформації в КС має охоплювати всі аспекти даної проблеми на усіх етапах їх життєвого циклу (розробка ТЗ, проектування і створення науково-технічної продукції в галузі ТЗІ, експлуатація, ремонт, модернізація, утилізація тощо), що досягається розробкою і реалізацією певної Відомчої програми стандартизації з комплексного технічного захисту інформації при її обробці в КС.

Метою такої пропонованої програми має бути створення комплекту нормативно-технічних документів, що регламентують норми, правила, технічні вимоги, методи контролю та випробувань, забезпечуючи розробку, виробництво, експлуатацію і ремонт технічних і програмних засобів відповідно до вимог захисту опрацьованої інформації. Вона має визначати перелік об'єктів стандартизації, а також компетенцію розроблених документів.

Система нормативних актів має включати декілька рівнів: стандарти з питань ТЗІ, керівні документи Кабінету міністрів України, міністерств та відомств з цього питання. Основу нормативного забезпечення складають стандарти з ТЗІ і керівні документи, розроблені за програмою стандартизації.

При проведенні заходів щодо захисту інформації в міжнародних КС і мережах ЕОМ необхідно керуватися як міжнародними нормами, так внутрішніми стандартами і правилами ТЗІ в Україні.

Для досягнення єдиної методології в галузі безпеки інформації в КС, має бути створено єдиний стандарт та низка документів, що охоплюють загальні положення, єдину класифікацію і термінологію, організацію робіт із створення, впровадження, сертифікації, експлуатації і розвитку комплексних систем захисту інформації (КСЗІ) як основи (ядра) безпеки КС, комплексу засобів захисту (КЗЗ) як основи ядра безпеки обчислювальної системи КС, а також визначення критеріїв їхньої ефективності і методів контролю [2]. Ці документи мають регламентувати права і обов'язки замовників, розробників, виготовлювачів і користувачів КС, а також визначати систему технічної документації КСЗІ та КЗЗ певних КС України відповідно до визначених їх рівнів, призначення та класів.

Усі стандарти ТЗІ мають відповідати міжнародній системі стандартизації у даній галузі.

Реалізація єдиної технічної політики у галузі безпеки інформації має здійснюватися групою нормативних документів, що включають:

- положення про реалізацію організаційних і організаційно-технічних заходів захисту об'єктів КС державних органів України;
- сучасні технічні вимоги до засобів захисту, реалізованим за кожним напрямком, насамперед в залежності від виду потенційних загроз;

- сучасні технічні вимоги до елементної бази і технології виробництва елементів КС, в т. ч. у захищеному виконанні.

У технічному завданні на науково-дослідні та дослідно-конструкторські роботи з захищених КС мають включатися вимоги на проведення аналізу можливих каналів витоку відомостей про зразки та засоби захисту, реалізовані протягом усього їх життєвого циклу в захищеній КС.

Питання захисту інформації мають бути виділені в спеціальний розділ приймальних випробувань КС. Методики випробувань мають розроблятися з урахуванням прийнятих моделей потенційних загроз і забезпечувати перевірку КС на відповідність вимогам стандартів ТЗІ та інших чинних нормативних документів.

Організаційні заходи захисту базуються на законодавчих актах і нормативних документах з технічного захисту інформації. Вони мають охоплювати всі основні шляхи зберігання інформаційного ресурсу і включати:

- обмеження фізичного доступу до об'єктів КС і реалізацію режимних заходів;
- режим та охорону приміщення, закладу;
- підбір обслуговуючого персоналу;
- встановлення юридичної відповідальності з забезпечення конфіденційності, цілісності, доступності, спостереженості та гарантованості критичної інформації;
- обмеження (виключення) можливості електромагнітного та інших видів безконтактного доступу або несанкціонованого впливу;
- обмеження інформаційного доступу до елементів КС шляхом запровадження правил розмежування доступу, криптографічним закриттям каналів передачі даних та сервісної інформації КС, виявленням і знищенням "закладок";
- створення твердих копій найбільш важливих з точки зору втрати масивів даних;
- проведення профілактичних та інших заходів від вкорінення комп'ютерних вірусів, особливо мережевих через Internet, Intranet, Extranet.

Нормативна документація на КСЗІ, КЗЗ має бути частиною експлуатаційної документації КС і мати обмеження з доступу до неї. До неї мають входити: настанова користувачу (у т. ч. програмісту) з застосування захисних механізмів і посібник з управління комплексною системою захисту інформації для власників (адміністрації) КС.

До комплекту документації КСЗІ, КЗЗ певної КС включаються також акти за результатами тестування (сертифікації) даної КС на захищеність.

Відповідальність за технічний захист та забезпечення безпеки критичної інформації в ході експлуатації КС покладається на керівництво підрозділів, які експлуатують дану захищену КС або її певний засіб, КЗЗ та КСЗІ, у тому числі з додержанням вимог щодо правового регулювання злочинів з використанням електронно-обчислювальних машин, комп'ютерних систем та мереж [3]. Доцільним, на наш погляд, у цій проблемі є поєднання зусиль фахівців технічного та правового напрямків забезпечення безпеки інформації в КС.

На основі викладеного вище можна зробити наступні висновки та пропозиції:

1. Нормативно-правові засади захисту інформації – це сукупність нормативно-правових актів та інших документів, дотримання вимог яких є обов'язковим для забезпечення безпеки інформації в захищених комп'ютерних системах.
2. Як свідчить досвід, успішність захисту інформації в комп'ютерних системах залежить від нормативно-правового забезпечення (до 60%), апаратно-програмного забезпечення (до 30%) та організаційних заходів (до 10%). Ця пріоритетність поступово, зі зростанням правової дисципліни персоналу комп'ютерних систем та досвіду їх експлуатації, перерозподіляється до апаратно-програмного забезпечення та оперативних організаційних заходів забезпечення безпеки.
3. На наш погляд, проблемним питанням залишається поєднання зусиль фахівців технічного та нормативно-правового забезпечення захисту інформації в комп'ютерних системах, адже мета у них одна – захист від злочинів з використанням електронно-обчислювальних машин, комп'ютерних систем та мереж [3].
4. Безумовно, попередження та розкриття злочинів з використанням електронно-обчислювальних машин, комп'ютерних систем та мереж і їх всебічне забезпечення з часом набуває не тільки практичного, але і теоретичного значення.

Література: 1 Барсуков В. С., Водолазкий В. В. Современные технологии безопасности. М.: издательство "Нолидж", 2000. С. 6–10. 2. Пакет нормативних документів з питань захисту інформації від несанкціонованого доступу Департаменту СТСЗІ СБ України (НД ТЗІ 1.1-002-99, НД ТЗІ 1.1-003-99, НД ТЗІ

2.5-004-99, НД ТЗІ 2.5-005-99), К., 1999. 3. Кримінальний кодекс України, розділ XVI, ст. 361, 362, 363, чинний з 01. 09. 2001 р.

УДК 12.00.04

ЗАХИСТ БАНКІВСЬКОЇ ТАЄМНИЦІ ПРИ ЗДІЙСНЕННІ ПРАВОСУДДЯ ГОСПОДАРСЬКИМИ СУДАМИ

Юрій Носік
Київський національний університет імені Тараса Шевченка

Анотація: **Розкрито й проаналізовано зміст, межі та процесуальний порядок охорони банківської таємниці в господарському судочинстві.**
Summary: **The substance, limits and the procedural order of bank secret preservation during the legal proceedings in the courts are outlined and analyzed in the article.**
Ключові слова: **Банківська таємниця, збереження банківської таємниці, господарсько-процесуальна охорона банківської таємниці, закрите судове засідання.**

І Правова модель охорони банківської таємниці в господарському судочинстві України

В господарському процесуальному законодавстві України передбачено унікальні правові засоби охорони банківської таємниці, які не повторюються в інших галузях процесуального права. *Закріплені в господарсько-процесуальному законодавстві правові норми спрямовані на охорону конфіденційної інформації банківського характеру і є складовою комплексної системи правової охорони банківської таємниці в Україні.*

Захист прав, свобод і законних інтересів учасників правовідносин як завдання господарського суду та законність як принцип його діяльності стосуються не тільки кінцевого результату здійснення правосуддя, а й усього процесу розгляду справ, включаючи, зокрема, і забезпечення збереження банківської таємниці при здійсненні правосуддя. Як відомо, банківською таємницею є інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту. Орієнтовний перелік відомостей, що становлять банківську таємницю, наведено в Законі України "Про банки і банківську діяльність" [1], проте остаточно з'ясувати, чи належать ті чи інші відомості до банківської таємниці можна тільки шляхом комплексного аналізу законодавства та врахування ряду фактичних обставин [2].

Процесуальною гарантією збереження банківської таємниці в господарському судочинстві є законодавчо забезпечена можливість розгляду господарських справ у закритих судових засіданнях. Зміст господарсько-процесуальної охорони банківської таємниці полягає в тому, що особам, які не беруть участі в судовому процесі, забороняється бути присутніми на судових засіданнях при розгляді справ, у матеріалах яких містяться відомості, що становлять банківську таємницю. Правова конструкція, яка спрямована на збереження банківської таємниці під час слухання справ у суді, закріплена в статті 4-4 Господарського процесуального кодексу України [3], гіпотезу і диспозицію якої необхідно розуміти так: ***коли розгляд справи у відкритому судовому засіданні господарського суду суперечить вимогам щодо охорони банківської таємниці, то розгляд такої справи відбувається в закритому судовому засіданні, про що постановляється ухвала***. Оскільки згідно з Законом України "Про банки і банківську діяльність" до банківської таємниці відносяться дані про стан рахунків, проведені операції і здійснені угоди, про організаційно-правову структуру юридичної особи, її керівників, напрями діяльності, то можна зробити висновок, що практично кожна справа в господарському суді має розглядатися в закритому судовому засіданні. Ця проблема потребує вивчення і з приводу неї має бути вироблена чітка позиція з боку судової практики.

Передбачений статтею 4-4 Господарського процесуального кодексу України (далі по тексту – ГПК України) відхід від принципу гласності розгляду справ у господарських судах з метою збереження банківської таємниці не суперечить закріпленим в Конституції та Законі України "Про судоустрій" [4] правовим засадам здійснення правосуддя в Україні, адже, згідно з частиною 3 статті 9 Закону України "Про судоустрій", випадки розгляду справ у закритих судових засіданнях мають встановлюватися саме процесуальним законом. Внесення норм щодо охорони банківської таємниці до Господарського процесуального кодексу України узгоджується також зі статтею 92 Конституції України, відповідно до якої