Ю.О. Коваленко

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Розвиток глобального процесу інформатизації суспільства, що спостерігається в останні десятиліття, спричинив нову глобальну проблему – інформаційну безпеку. Багато найважливіших інтересів підприємства в даний час значною мірою визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки. Тому інформаційна безпека в сучасних умовах є однією з необхідних умов нормального функціонування підприємства.

Усе більш очевидною стає залежність загального рівня економічної безпеки підприємства від інформаційної складової. Практика показує, що будь-яка недружня акція, спрямована проти інтересів господарського суб'єкта, починається зі збору інформації: навіть дрібне розкрадання звичайно випереджає вивчення особою зі злочинними задумами можливості протиправних дій, і без відповідного інформаційного забезпечення не представляються такі деструктивні прояви, як відведення активів підприємства або рейдерське захоплення.

Не випадково питання інформаційної безпеки вже давно входять до головних пріоритетів практично всіх великих компаній. Останнім часом більше керівників середнього і малого вітчизняного бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією, системами її обробки і співробітниками, що беруть участь у цьому процесі.

Питання інформаційної безпеки знайшли відображення у таких законах України: «Про основи національної безпеки України» [3], «Про концепцію національної програми інформатизації» [1], «Про національну програму інформатизації» [2], а також у Стратегії національної безпеки України, яка затверджена Указом Президента [5].

У Законі «Про основи національної безпеки України» надано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України.

У Стратегії національної безпеки, присвяченій стану інформаційної безпеки в нашій державі, зазначено:

посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності;

недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту;

наближається до критичного стан безпеки інформаційно-комп'ютерних систем у фінансовій і банківській сфері, сфері державного управління, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо [5, п. 2.8].

Поняття інформаційної безпеки можна розглядати у декількох ракурсах. По-перше, це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави. По-друге, це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їх існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і, як наслідок – обгрунтованість подальших рішень і дій.

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави, акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

© Коваленко Юлія Олександрівна – кандидат економічних наук, доцент.
Донецький юридичний інститут ЛДУВС ім. Е.О. Дідоренка.

Зі зростанням науково-технічного прогресу буде зростати важливість питання інформаційної безпеки. Інформація стала чинником, який може призвести до значних технологічних аварій, військових та політичних конфліктів, дезорганізувати державне управління, фінансову систему. Чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав усе більше здійснюється за допомогою інформатизації. Ураховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися кругозір та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і суперечать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [10, *35-38*].

З огляду на це можна констатувати нове розуміння проблем інформаційної безпеки. Так, Б. Кормич трактує інформаційну безпеку як стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів та відносин [9, *15*]. Деякі вчені розглядають інформаційну безпеку як такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання шкоди через неповноту, несвоєчасність, недостовірність інформації чи негативний інформаційний вплив, через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [6, *72*]. Інформаційну безпеку суспільства також визначають як неможливість завдання шкоди його духовній сфері, культурним цінностям, соціальним регуляторам поведінки людей, інформаційній інфраструктурі й повідомленням, що передаються за її допомогою [7, *64*].

Науковці стверджують, що передбачити всі можливі загрози у сфері інформаційної безпеки неможливо, оскільки вони здатні міняти свої зміст і динаміку, а правове регулювання потребує стабільності [9, *16*]. Саме тому наголошується на необхідності спрямовувати політику інформаційної безпеки не на пошук відповіді на певну загрозу, а на створення безпечних умов функціонування інформаційної сфери, за яких вона буде несприйнятливою до можливих негативних впливів.

Фахівцями термін «інформаційна безпека» розуміється по-різному, причому найчастіше мається на увазі якийсь один аспект цієї проблеми. Наприклад, з погляду керівника підприємства серйозну загрозу становить крадіжка секретної документації, з позиції розроблювача антивірусних програм – ризик знищення безцінних даних. Кожний із цих аспектів заслуговує окремого вивчення, але для споживача важливо забезпечити безпеку взагалі, а не тільки за окремими ризиками.

На нашу думку, інформаційна безпека для підприємства полягає у певних діях щодо вияву, усунення та нейтралізації негативних джерел, причин і умов впливу на інформацію.

При цьому поняття «інформаційна безпека» характеризує стан інформаційного захисту господарюючого суб'єкта, в умовах якого можлива дія загроз. Досягається це системою заходів, спрямованих на попередження, вияв та ліквідацію інформаційних загроз.

Мета статті полягає в розробці основних заходів щодо попередження виникнення загроз втрати, знищення інформації та забезпечення інформаційної безпеки на підприємстві.

Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, вірогідність тощо, може призвести до досить негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами; розголошення відомостей, що становлять комерційну й інші види таємниць; порушення вірогідності фінансової

документації; несанкціонованого доступу до персональних даних фізичних осіб тощо. Результатом перерахованого можуть стати: погіршення ділових відносин із партнерами; зриви переговорів, втрата вигідних контрактів; невиконання договірних зобов'язань; необхідність проведення додаткових ринкових досліджень; відмовлення від рішень, що стали неефективними через розповсюдження інформації, і, як наслідок, – фінансові втрати, пов'язані з новими розробками; втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію; зниження цін або обсягів реалізації; втрати ділової репутації; більш жорсткі умови одержання кредитів; труднощі в постачанні і придбанні устаткування тощо. У визначених ситуаціях зневага питаннями захисту інформації може призвести до повного банкрутства.

Тому питання аналізу загроз і ризиків є визначальним при побудові ефективної системи захисту інформації. Однак, за оцінками фахівців, лише не більше 5% підприємств використовують власні методики аналізу ризиків, що дозволяють виконувати кількісний аналіз та оптимізацію підсистеми інформаційної безпеки.

Водночас дії внутрішніх порушників, такі як недбалість співробітників, крадіжки інформаційних ресурсів та IT-устаткування, фінансові й інші види шахрайства з використанням інформаційних систем і ресурсів тощо, набагато рідше стають предметом уваги при розв’язанні проблем інформаційної безпеки у випадку, якщо вони розглядаються у відриві від загальних завдань забезпечення економічної безпеки. Результати досліджень показують, що більшість підприємств не вживають достатніх заходів для захисту від дій інсайдерів.

Статистика у сфері інформаційної безпеки свідчить, що близько 80% зловмисників належить до інсайдерів. У компаніях телекомунікаційної галузі на їх дії припадає близько 90% фінансових утрат.

Людський фактор завжди був і є одним із найважливіших ризиків будь-якого бізнесу, оскільки більшість інцидентів відбуваються саме з вини співробітників. Навмисний відплив часто важко відрізнити від ненавмисного, однак це не завжди потрібно, оскільки наслідки для підприємства при будь-якому із цих варіантів можуть бути катастрофічними. Те, що більшість керівників не знають джерел внутрішніх загроз, говорить про те, що бізнесом приділяється недостатньо уваги інформаційній безпеці, що, утім, є одним із найважливіших факторів існування підприємства.

Аналіз, проведений на підприємствах середнього бізнесу, показав, що випадкові кібер-атаки виникають частіше і потенційно можуть нашкодити більше, ніж навмисні атаки інсайдерів. У результаті дослідження з'ясовано, що більшість підприємств приділяють набагато більше уваги захисту від навмисних внутрішніх атак, ніж від більш частих і потенційно більш руйнівних випадкових внутрішніх інцидентів.

Поза увагою залишаються питання потенційних внутрішніх ризиків, що виходять від співробітників, які мають доступ до критично важливих систем і секретної інформації. Хоча керівники усвідомлюють існування таких ризиків, турбота про зовнішню інформаційну безпеку часто переважує інші питання. Але значною є кількість порушень та випадків несанкціонованого доступу і використання інформації самими співробітниками, що ставить під загрозу основу бізнесу багатьох підприємств.

Із 500 керівників підприємств у сфері IT, що брали участь у дослідженні, більшість відзначили, що вони не знають джерел і причин виникнення внутрішніх загроз. При цьому підприємства намагаються оцінити потенційний фінансовий збиток від цих загроз та їх вплив на операційну діяльність. Половина опитаних упевнені, що більшість внутрішніх загроз створюється ненавмисно, 20% вважають загрози навмисними, 25%, – що навмисних і ненавмисних загроз приблизно нарівно, 5% утруднилися з відповіддю. Однак у пункті, де пропонувалося перелічити найбільші загрози за їх важливістю, майже 85% респондентів не могли точно сказати, чи були навмисними

або випадковими внутрішні інциденти, спровоковані підрядчиками або тимчасовими співробітниками.

Дослідження також показало, що приблизно раз на місяць на підприємствах трапляється один інцидент, який можна віднести до одного з 10 можливих типів загроз. Більше за все відбувається випадків ненавмисної втрати даних через недбалість співробітників – таких інцидентів відбувається 15-20 на рік. Внутрішні зловмисні атаки і шпигунство – 10 випадків на рік, зловживання доступом до інформації – 20 випадків на рік. Якщо говорити про сферу діяльності, то на досліджуваних підприємствах відбувається до 20-30 інцидентів щорічно. Результати дослідження свідчать, що універсального рішення для усунення внутрішніх ризиків не існує. Кожне підприємство має виробити власний комплексний підхід з урахуванням особливостей структури і специфіки діяльності.

Хоча навмисних атак зловмисників стає все більше, практика показує, що випадкові помилки, неуважність до правил безпеки впливають на діяльність підприємства набагато більше, ніж атаки шахраїв.

Фахівці у сфері інформаційної безпеки дотримуються двох думок. Перша полягає у такому: інформаційною безпекою на підприємстві можна взагалі не займатися, не витрачаючи коштів. У цьому випадку не виключений такий варіант, що прийнятий ризик себе цілком виправдає. Другий погляд: необхідно витратити на створення системи захисту інформації чимало грошей (навчання персоналу, програмне забезпечення тощо) і тим самим забезпечити належний рівень безпеки. Але при цьому також залишиться деяка вразливість, що рано або пізно призведе до відпливу або розкрадання конфіденційної інформації.

В обґрунтуванні витрат на інформаційну безпеку можна використати нижченаведений підхід. Необхідно застосувати на практиці інструментарій визначення рівня інформаційної безпеки. Керівництво підприємства залучається до оцінки вартості інформаційних ресурсів, визначення оцінки потенційного збитку від порушень інформаційної безпеки. Від результатів цих оцінок буде багато в чому залежати подальша діяльність керівників у сфері інформаційної безпеки. Якщо інформація нічого не коштує, істотних загроз для інформаційних активів немає, а потенційний збиток мінімальний, то проблемою забезпечення інформаційної безпеки можна не займатися. Якщо ж інформація має значну вартість, загрози і потенційний збиток ясні, тоді постає питання про внесення в бюджет витрат на підсистему інформаційної безпеки. У цьому випадку слід заручитися підтримкою керівництва підприємства в усвідомленні проблем інформаційної безпеки й побудові системи захисту інформації.

Надійно гарантувати бізнес від перерахованих негативних явищ можна тільки на основі формування ефективної системи забезпечення інформаційної безпеки.

Однак тут існують певні проблеми, що належать, швидше за все, до організаційно-фінансових. Першою і найбільшою проблемою у створенні системи інформаційної безпеки є відсутність розуміння в керівництва необхідності створення такої системи. Багато керівників підприємств не усвідомлюють, що створювати систему інформаційної безпеки просто необхідно, бо своєчасне створення її позбавить підприємство збитків, а іноді навіть і врятує бізнес.

Друга проблема при створенні системи інформаційної безпеки – відсутність достатньої кількості фінансових коштів. Відсутність фінансування з мінімального бюджету для створення системи інформаційної безпеки зустрічається також дуже часто. Приміром, у США і країнах Євросоюзу на створення системи інформаційної безпеки і підтримку її в актуальному стані виділяється від 30% прибутку компанії. В Україні ж якщо фінанси і виділяються, то разово й у недостатній кількості. Їх може вистачити хіба що на продовження ліцензії на антивірус. І лише деякі підприємства, які можна вважати скоріше винятком із правил, планують і приймають бюджет своєї системи інформаційної безпеки виходячи з реальних

потреб.

Третьою найнебезпечнішою проблемою є ситуація, коли є розуміння керівництва та необхідні кошти, але створення системи інформаційної безпеки доручають фахівцям, що не мають ані відповідної освіти, ані достатнього досвіду. Найчастіше це бувають системні адміністратори або відділ технічної підтримки. Вони, у свою чергу, розцінюють це як установку і налаштування антивірусу. Наявність внутрішнього зловмисника, найчастіше, узагалі не береться до уваги. Відповідно до статистики 70% порушень здійснюється внутрішніми зловмисниками. Ще частіше без належної уваги залишаються канали зв'язку, і переписка керівництва підприємства з діловими партнерами, із клієнтами стає незахищеною. У результаті таких дій кошти витрачені, а інформаційна безпека на колишньому рівні.

Багато керівників підприємств можуть не бачити очевидного зв'язку між утратою доходів і відсутністю фінансових ресурсів у системі інформаційного захисту. Тому в першу чергу необхідно подати проблему у зрозумілому для бізнесу вигляді. Це завдання лягає на керівництво служби інформаційної безпеки господарюючого суб'єкта, що має виявити і наочно показати власникам підприємства весь спектр загроз в інформаційній сфері, а також переконати, що протистояти їм можна тільки на основі створення і упровадження ефективних систем захисту інформації.

Створюючи такі системи, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різнорідних заходів, які можна розділити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, кінцевий успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки.

У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями:

розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;

організація і здійснення конкретних видів діяльності із захисту інформації;

експлуатація технічних засобів захисту інформації;

аудит і контроль функціонування системи інформаційної безпеки підприємства.

У рамках першого напряму мають розв’язуватися такі основні завдання:

аналіз і узагальнення потенційних загроз і таких, що реалізувалися, причин порушень вимог інформаційної безпеки. Аналіз ступеня забезпечення безперервності бізнес-процесів, що використовують ІТ, з точки зору інформаційної безпеки. Пошук нових загроз і вразливостей, пов'язаних з інформаційною взаємодією;

побудова методик оцінки інформаційних ризиків;

інформаційне обстеження підприємства та інформаційних ресурсів;

розробка методів захисту інформації та ІТ і методик їх упровадження в діяльність підприємства;

розробка і модифікація концепції та політики забезпечення інформаційної безпеки. Створення локальної нормативної бази із цих питань з урахуванням комплексного підходу до економічної безпеки;

розробка методик оцінки рівня інформаційної безпеки і визначення достатності захисту інформації та ІТ з урахуванням потреб бізнесу, а також існуючої і перспективної нормативної бази;

аналіз виконання вимог інформаційної безпеки всіх використовуваних процедур

створення, обробки, пересилання, збереження, знищення інформації, у тому числі: процедур інформаційної взаємодії підрозділів підприємства між собою і із зовнішніми організаціями; порядків доступу співробітників підприємства і суміжних організацій, а також клієнтів до інформаційних ресурсів і зовнішніх комп'ютерних мереж; проектів розвитку IT, включаючи системи зв'язку і телекомунікацій; проектів договорів із зовнішніми організаціями, з якими здійснюється обмін інформацією; проектів інших нормативних документів, що передбачають інформаційну взаємодію;

підготовка аналітичних записок, що містять висновки із проведеного аналізу і пропозиції щодо реалізації захисту інформації.

Другий напрям передбачає такі основні завдання:

планування на основі координації діяльності всіх підрозділів робіт із забезпечення інформаційної безпеки підприємства;

організація й участь у впровадженні методів забезпечення інформаційної безпеки в діяльність підприємства. Робота з персоналом, партнерами і клієнтами;

узгодження заявок на доступ і порядку доступу співробітників і зовнішніх організацій до інформаційних ресурсів підприємства; процедур інформаційної взаємодії підрозділів із зовнішніми організаціями; договорів, з якими здійснюється інформаційна взаємодія; проектів наказів, розпоряджень, інших нормативно-розпорядницьких документів;

розв’язання поточних практичних питань з інформаційної безпеки, що виникають у підрозділах.

У рамках третього напряму мають розв’язуватися такі основні завдання:

підтримка ключових структур, використовуваних у зовнішніх і вбудованих засобах криптографічного захисту інформації;

підтримка роботи інших засобів інформаційної безпеки.

Четвертий напрям передбачає розв’язання таких основних завдань:

перевірка виконання вимог інформаційної безпеки працівниками підприємства й іншими особами, що мають доступ до інформаційних ресурсів;

моніторинг дій користувачів IT (несанкціонованої модифікації інформації, використання різних поштових та інших сервісів мережі Інтернет для відправлення конфіденційної інформації за межі підприємства тощо);

контроль своєчасної зміни прав користувачів в інформаційних системах; блокування облікових записів звільнених (переведених на іншу роботу) користувачів; контроль дотримання настроювань безпеки, включаючи парольну політику, інші вбудовані системи інформаційної безпеки, зовнішні засоби захисту інформації;

моніторинг роботи систем виявлення (запобігання) мережних атак, систем оцінки якості побудови мережі й інших автоматизованих систем комп'ютерної безпеки;

участь у розборі виявлених порушень інформаційної безпеки і вимог нормативних документів із цих питань. Підготовка пропозицій щодо попередження порушень;

проведення внутрішнього аудиту питань інформаційної безпеки. Підготовка пропозицій щодо використання зовнішнього аудиту;

проведення моніторингу можливого випливу конфіденційної інформації технічними каналами.

З огляду на міждисциплінарний характер питань, що входять у блок інформаційної безпеки, деякі з перелічених функцій можуть виконуватися тільки разом з іншими структурними службами підприємства (службою по роботі з персоналом, юридичною, господарською службою тощо).

Для цього необхідно визначити політику безпеки підприємства – сукупність керівних принципів, правил, процедур і практичних прийомів сфери інформаційної безпеки, що регулюють управління, захист і розподіл цінної інформації на підприємстві.

У загальному випадку такий набір правил становить деяку функціональність програмного продукту, необхідного для його

використання в конкретній організації. Якщо підходити до політики безпеки більш формально, то вона є набором певних вимог до функціональності системи захисту, закріплених у відомчих документах.

Головною причиною появи політики безпеки звичайно є вимога наявності такого документа від організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

Крім того, визначені вимоги та рекомендації ставлять галузеві або загальні, місцеві або міжнародні стандарти. Звичайно це виражається у вигляді зауважень зовнішніх аудиторів, що проводять перевірки діяльності підприємства. Відсутність політики спричиняє негативну оцінку, що у свою чергу впливає на публічні показники підприємства – позиції в рейтингу, рівень надійності тощо.

Далі випливає з'ясування, наскільки серйозні втрати може принести підприємству настання інформаційного ризику на кожен конкретний інформаційний об'єкт. Існує безліч схем обчислення ризиків, варто зупинитися на одній із найпростіших.

Втрати від настання інформаційного ризику можуть бути подані у такий спосіб:

Величина ризику	Опис
0,1-0,2	Оголошення інформації принесе незначні моральні і фінансові втрати підприємству
0,2-0,3	Втрати від інформаційної атаки є, але вони незначні, основні фінансові операції і становище підприємства на ринку не порушено
0,3-0,4	Фінансові операції не ведуться протягом деякого часу, за цей час підприємство зазнає збитків, але його становище на ринку і кількість клієнтів змінюються мінімально
0,4-0,6	Значні втрати на ринку й у прибутку. Підприємство втрачає значну частину клієнтів
0,6-0,8	Втрати дуже значні, підприємство на період до року втрачає становище на ринку. Для відновлення становища потрібні великі фінансові інвестиції
0,8-1,0	Підприємство припиняє існування

Необхідно відзначити, що класифікацію збитку, нанесеного атакою, має оцінювати власник інформації або працюючий із нею персонал. Оцінку ймовірності появи атаки краще довіряти технічним співробітникам підприємства.

З різних організаційних схем функціонування підрозділів, що відповідають за інформаційну безпеку підприємства (функції такого підрозділу покладаються на системних адміністраторів; зазначений підрозділ знаходиться у структурі служби інформаційної безпеки, що підкоряється вищому керівництву), найкращим є варіант, при якому підрозділ інформаційної безпеки входить до складу служби економічної безпеки підприємства. Саме в цьому випадку створюються найкращі можливості розв’язання проблем інформаційної безпеки в контексті загальних завдань безпеки бізнесу.

Висновки. Таким чином, у сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. У свою чергу, надійне забезпечення інформаційної безпеки є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. На наш погляд, особливої уваги потребує реальне втілення запропонованих заходів щодо забезпечення інформаційної безпеки, які мають стати основою для формування та реалізації інформаційної політики підприємства, захисту інформації від внутрішніх та зовнішніх загроз.

Література

1. Про концепцію національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 182.

2. Про національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 181.

3. Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

4. Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні: Постанова Верховної Ради України від 1 грудня 2005 року // Відомості Верховної Ради України. – 2006. – № 15.

5.Про Стратегію національної безпеки України: Указ Президента України від 12 лютого 2007 року № 105/200 // Офіційний вісник України. – 2007. – № 11. – Ст. 389.

6. Баранов А. Інформаційний суверенітет або інформаційна безпека? / А. Баранов // Національна безпека та оборона. – 2001. – № 1. – С. 70-76.

7. Иванов О.В. Информационная составляющая современных войн / О.В. Иванов // Вестн. Моск. ун-та. Сер. 18: Социология и политология. – 2004. – № 4. – С. 64-70.

8. Інформаційне законодавство: зб. законодавчих актів у 6 т. / за заг. ред. Ю.С. Шемшученка, К.С. Чижа. – Т. 5: Міжнародно-правові акти в інформаційній сфері. – К.: Юридична думка, 2005. – 328 с.

9. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ... д-ра юрид. наук / Б.А. Кормич. – Харків, 2004. – 44 с.

10. Роговец В. Информационные войны в современном мире: причины, механизмы, последствия / В. Роговец // Персонал. – 2000. – № 5. – С. 34-40.

11. Рощин С.К. Психологическая безопасность: новый подход к безопасности человека, общества и государства / С.К. Рощин, В.А. Соснин // Российский монитор. – 1995. – № 6 [Электронный ресурс]. – Режим доступа: http://www.bookap.by.ru/psywar/grachev/gl6. shtm.