задачі: обробку даних, обробку інформації, реалізацію інтелектуальної діяльності з метою створення інформації. Управлінські інформаційні системи послідовно реалізують принципи єдності виробничого процесу та інформаційного процесу супроводу через застосування технічних засобів збору, нагромадження, обробки і передачі інформації в поєднанні з використанням аналітичних методів математичної статистики і моделей прогнозно-аналітичних розрахунків та інших необхідних прикладних засобів. Підвищення ефективності використання інформаційних систем досягається шляхом наскрізної структури і сумісності інформаційних систем, які дозволяють усунути дублювання і забезпечують багатократне використання інформації, встановлюють визначені інтеграційні зв'язки, обмежують кількість показників, зменшують обсяг інформаційних потоків, підвищують рівень використання інформації. Тому можна сказати, що подальший розвиток забезпеченості підприємств сільського господарства інформацією, підтримка цієї сфери законодавством призведе до подальшого перспективного розвитку сільського господарства і економіки в цілому.

Література:

1. Вісник аграрної науки Причорномор'я – 2005. - №5
2. Вісник аграрної науки. – 2007. - №6.
3. Економіка АПК – 2006. -№8

ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНИХ УМОВАХ

Фурман Т.М.
Наукові керівники:
доцент **Киш Л.М**.
асистент **Гапчак Т.Г.**

Визначено основні аспекти інформаційної безпеки в сучасних умовах, а також характеристику причин, що призводять до виникнення інформаційних війн.

Постановка проблеми. Проблема захисту інформації набула особливо вагомого значення в наш час. Тепер багато фізичних та юридичних осіб використовують комп'ютер для зберігання даних та обміну ними. При цьому існує досить багато зловмисників, що хочуть отримати ту чи іншу інформацію незаконним шляхом

Захист інформаційного суверенітету тісно пов'язаний із поняттям інформаційної безпеки, що може бути розглянута, як захищеність внутрішньої інформації як такої, що припускає захищеність якості інформації, її надійність, захищеність різних галузей інформації (державної, банківської, комерційної таємниці) від розголошення, захищеність інформаційних ресурсів.

Слід відмітити, що в силу суб'єктивних факторів категорія „інформаційна безпека" сьогодні розглядається в Україні і за кордоном переважно у організаційно-управлінському та інженерно-технологічному аспектах, що не зовсім правильно і в майбутньому може призвести до неправильного формування державної політики. Відразу зауважимо, що зазначені аспекти є важливими у системі організації захисту інформації, але без правового аспекту вони не можуть претендувати на системність і комплексність безпеки [3].

Ціль роботи. Основна мета – створення умов, які б забезпечили належне зберігання і захист інформації в сучасних умовах.

Виклад основного матеріалу. Виходячи з правового аналізу інформаційного законодавства України, інформаційна безпека виступає одним із багатьох його провідних багатоаспектних чинників (об'єктом правовідносин). Таким чином, можна подати зміст інформаційної безпеки у контексті окремих організаційно-правових аспектів наступним чином. Інформаційна безпека – це суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини пов'язані із організацією технологій створення, розповсюдження, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави.

Тривалий час методи захисту інформації розробляли лише державні органи, а їх впровадження розглядалось як виключне право тієї чи іншої держави. Однак в останні роки з розвитком комерційної та підприємницької діяльності збільшилась кількість спроб несанкціо-

нованого доступу до конфіденційної інформації, а проблеми її захисту стали у центрі уваги багатьох учених та фахівців різних країн. Внаслідок цього з'явилася низка відкритих публікацій про дослідження та розробки в цій галузі, значно зросла потреба у фахівцях із захисту інформації.

Але, все ж таки як би не намагалися спеціалісти по інформаційній безпеці, які б „хитроумні" пристрої чи моделі розвитку вони не створювали, повністю виключити вірогідність порушення безпеки інформації вони не зможуть [1].

Сучасні війни ведуться перш за все в інформаційній сфері, яка випереджає і безперервно супроводжує так званий "прямий контакт" протиборчих сторін. Спецслужби ведуть свої війни безпосередньо в Інтернеті. Як повідомлялося, для боротьби з потенціальним супротивником в експортне мережене обладнання США встановлюються чіпи з логічними вірусами, які можуть бути активізовані в потрібний момент. Для боротьби з певними людьми є комп'ютерні програми обнуління банківських рахунків. І мабуть, багато що є ще, про що ми й не знаємо и маємо тільки здогадуватись.

Головне завдання інформаційних воєн полягає у маніпулюванні масами, у впливі на еліту певних держав або й своєї країни. Мета такої маніпуляції найчастіше полягає у: внесенні у суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів; дезорієнтації та дезінформації мас; послабленні певних переконань, устроїв; залякуванні свого народу образом ворога; залякуванні супротивника своєю могутністю.

Мета інформаційної війни, може включати будь-який елемент у епістемології супротивника. Епістемологія містить у собі організацію, структуру, методи і вірогідність знань. На стратегічному рівні ціль кампанії інформаційної війни – вплинути на рішення супротивника, і як наслідок, на його поводження таким чином, щоб він не знав, що на нього впливали. Навіть тоді, коли цієї мети важко досягти, вона все-таки залишається кінцевою метою кампанії на стратегічному рівні. Успішна, хоча і незавершена інформаційна кампанія, проведена на стратегічному рівні, приведе до рішень супротивника (а отже і його дій), що будуть суперечити його намірам чи заважати їхньому виконанню.

Захист інформаційного суверенітету тісно пов'язаний із поняттям інформаційної безпеки, що може бути розглянута, з одного боку, як захищеність внутрішньої інформації як такої, що припускає захи-

щеність якості інформації, її надійність, захищеність різних галузей інформації (державної, банківської, комерційної таємниці) від розголошення; захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії.

Ще одним важливим аспектом інформаційної безпеки є захист комп'ютерної інформації від розкрадань. Державна політика забезпечення інформаційної безпеки, будучи складовою частиною політики національної безпеки, припускає системну превентивну діяльність органів влади щодо забезпечення гарантій інформаційної безпеки особистості, соціальних груп і суспільства в цілому.

Існує багато різних засобів несанкціонованого доступу до інформації. Але слід одразу ж відмітити, що ніякий окремо взятий засіб захисту не в змозі гарантувати адекватну безпеку. Надійний захист можливий лише за умови створення механізму комплексного забезпечення безпеки. Можна виділити три основні складові такого комплексу: нормативно-правові; технічні; організаційні засоби [2].

Таким чином, інформаційна безпека не зводиться до комп'ютерної безпеки, як, утім, і поняття інформатизації не зводиться до поняття комп'ютеризації. Комп'ютерна безпека стосується лише охорони устаткування і інформації в ЕОМ від саботажу, порушення правил технічної експлуатації, присвоєння майна, стихійних лих, нанесення навмисного чи випадкового збитку і т.д. Інформаційна безпека, включаючи в себе комп'ютерну безпеку в якості необхідної складовий, поширюється на всі соціальні процеси, у яких функціонує інформація і використовується інформатика. Іншими словами, інформаційна безпека поширюється на всі явища інформаційної сфери соціуму (цивілізації), що прямо чи опосередковано "працюють" на оптимальний розвиток суспільної системи, забезпечуючи останньої умови для виживання і послідовного прогресу [1].

Випадків, що носять протиправний і аморальний характер, безліч. Насамперед це „електронні" крадіжки, тобто крадіжки грошей за допомогою ЕОМ.

На конференції по безпеці інформаційних систем у Мадриді генеральний директор однієї з корпорацій сказав, що фахівець з інформатики – це людина з дуже розвитим розумом, і якщо вона виявляється одержимо якою-небудь ідеєю, віна здатна зробити речі, воісти-

ну гідні Макіавеллі. Тільки банки США втрачають десятки мільярдів доларів на рік, що порівняно з економічними перевагами від використання комп'ютерів, причому вже половина злочинів у діловому світі пов'язана з застосуванням інформаційних технологій.

Серед інших негативних наслідків інформатизації, викликаних порушенням інформаційної безпеки, – комп'ютерний тероризм і комп'ютерне хуліганство. "Телефонний фанатик", „хакер", „крекер" – вираження сьогоднішнього лексикона. Якщо хакери проникають у пам'ять комп'ютеризованих систем для задоволення особистих амбіцій, то крекери ще і "викачують" інформаційні банки. Подібні "фахівці" катастрофічно небезпечні для комп'ютерних систем, керуючих бойовими ракетами, космічною і ядерною зброєю. До яких наслідків може привести їхнє "професійне" втручання, догадатися неважко. Це може стати трагедією не тільки для однієї країни, але і для всього людства.

Дуже тривожним моментом у забезпеченні інформаційної безпеки громадян є "електронне стеження", тобто запис і прослуховування телефонних розмов, перлюстрація листів і інші методи поліцейського контролю. За допомогою особливих програм комп'ютери можуть порівнювати й оцінювати працівників, підготовляти списки для чи звільнення заохочення. Позитивне для підприємця обертається негативним для робітників та службовців [3].

Україна, з огляду на її геополітичне положення, цілком може використовуватися як своєрідний полігон боротьби національних інтересів ведучих країн світу. Крім того, на чисто політичні моменти органічно накладаються і загальносвітові тенденції діалогу країн "першого" і "третього" світу. Ні для кого не секрет, що існуючі могутні політичні сили, що намагаються забезпечити соціально-економічну стабільність у розвинутих країнах за рахунок закріплення їхнього пануючого положення у світі, нарощування розриву з непривілейованою більшістю. При цьому, якщо раніш, у колоніальну епоху, основний розрахунок будувався на моці збройних сил, то в наш час розвинуті країни орієнтовані на економічне панування, експлуатацію ресурсів інших народів і використовують в основному невоєнні засоби: формування в цих країнах маріонеткових компрадорських еліт, морально-духовне поневолення через тиражовані ЗМІ зразки псевдокультури.

Особливості розвитку світу інформації, можливості необмеженого та неконтрольованого впливу, несанкціонований доступ,

комп'ютерні віруси та т. ін. гостро поставили перед суспільством проблеми інформаційної безпеки, яка повинна здійснюватися комплексно та систематично з використанням різних засобів (апаратних, програмних) щоби запобігти інформаційному тиску та в цілому будь-якій іншій інформативній небезпеці [4].

Висновки. Інформаційні системи все більше ускладнюються, взаємозалежність між різноманітними компонентами вже не завжди очевидна та інформаційна безпека набуває таким чином все більш глобального характеру, виходячи у більшості випадків на перший план.

В сучасних ринкових умовах господарювання інформаційна безпека в умовах глобального інформаційного суспільства відіграє провідну роль. Широка інформатизація всіх сфер життя суспільства, зокрема сфери забезпечення безпеки особи, суспільства, економіки і фінансів, державної інфраструктури, ставить питання про комплексний підхід до проблеми інформаційної безпеки.

Література:

1.Абрамович К. Л. Місце інформаційної безпеки у розвитку інформаційного суспільства // Формування ринкових відносин в Україні. – 2007. – №9. – с. 110-113.

2. Градісов В. М. Інформаційна безпека та ефективність державного управління // Підприємство, господарство і право. – 2004. – №3. – с. 88-91.

3. Кириленко М.Л. Формування інформаційного простору у сучасних умовах // Інвестиції: практика та досвід. – 2007. – №16. – с. 40-43.

4. Ткаченко А. М. Інформатизація як конкурентна перевага підприємства // Актуальні проблеми економіки. – 2004. – №1. – с.147-154.

ПОЗИКОВА ФОРМА ПРАЦІ В УКРАЇНІ ТА ЇЇ ВИДИ

Карнафель В.
Науковий керівник: