Угрозы **конфиденциальности** направлены на запрещенное режимом доступа перемещение информации от носителя-источника к носителю-получателю.

Информация сохраняет конфиденциальность, если соблюдается, прежде всего, согласно сформулированной парадигме, режимная адекватность носителей информации.

Угрозы **целостности** информации направлены на запрещенное режимом доступа (порядка получения, использования, распространения и хранения информации) ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно, а также в результате объективных воздействий со стороны среды, окружающей носитель информации.

Информация сохраняет целостность, если соблюдаются, в соответствии со сформулированной парадигмой, установленная режимная адекватность относительно правил ее модификации (удаления).

Любой субъект, воздействующий на носитель-источник информации с целью модификации информации, можно рассматривать как **носитель** информации, несущей в себе представление о необходимой модификации (удалении) информации носителя-источника информации. В процессе модификации происходит перемещение модифицирующей информации.

Воздействие объектов, процессов, окружающей среды и других факторов, которые часто относят к разряду "случайных" – это несоответствие носителя-источника информации установленному режиму доступа, часто приводящее к нарушению коммуникабельности. Данное воздействие является нарушением режимной адекватности, как следствие, коммуникабельности носителей информации.

Угрозы **доступности** (отказ в обслуживании) направлены на преднамеренное или непреднамеренное нарушение коммуникабельности носителей информации при их взаимодействии. Нарушение коммуникабельности прерывает разрешенные режимом доступа процессы перемещения информации.

Информация сохраняет доступность, если сохраняется коммуникабельность носителей информации при их взаимодействии.

Выводы

Сформулированная парадигма (которая может интерпретироваться как общий закон, аксиома или основное правило) выносится на обсуждение с целью проверки ее на соответствие всем современным аспектам информационной безопасности.

В случае успешной апробации данная парадигма может стать краеугольным камнем, вокруг которой возможно построение и эффективное развитие теоретико-методологических основ обеспечения безопасности информации, основное содержание которых приведено во введении к данной статье. В первую очередь видится необходимость переработки нормативно-методической базы, касающейся информационной безопасности, а потом и коррекция созданных и построение новых комплексных систем защиты информации.

Авторы ждут отзывов, критических замечаний и рекомендаций от всех заинтересованных лиц и организаций.

Литература: 1. Безопасность информационных технологий. Методология создания систем защиты/ В. В. Домарев. – К.: ООО "ТИД "ДС", 2001. – 688 с. 2. Советский энциклопедический словарь/ Гл. ред. А. М. Прохоров 4-е изд. – М.: Сов. энциклопедия, 1989, – 1632 с. 3. НД ТЗИ 1.1 – 002 – 99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. Нормативный документ ДСТЗИ СБ Украины. Киев, 1999. 4. Закон України "Про інформацію" № 2657–XII від 02. 10. 92р.

УДК 002.6+342.7

ДЕЯКІ ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ ВЗАЄМОВІДНОСИН ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Володимир Гурковський

Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

Анотація: **Пропонуються організаційно-правові заходи щодо координації боротьби з комп'ютерними правопорушеннями.**

Summary: **The organization-legal measures on coordination of struggle with computer offences are offered.**
Ключові слова: **Взаємовідносини, взаємодія, координація, комп'ютерна злочинність, інформаційна безпека.**

I Вступ

Українське суспільство знаходиться на стадії розвитку, що характеризується етапом вдосконалення функціонування державного апарату та механізму здійснення державного управління в певних сферах життєдіяльності. В зв'язку з цим в системах, структурах, їх правовому статусі та методах здійснення державної влади мають відбуватися якісні зміни.

Однак, українське суспільство ще не має достатнього організаційно-управлінського досвіду, його організаційний потенціал низький [1].

В зв'язку з цим важливим завданням науки державного управління є вивчення, узагальнення (з метою приведення апарату у відповідність з новими потребами держави) та ліквідація в апараті управління процесів, що не відповідають умовам та вимогам сучасного розвитку державності.

Оптимізація системи державного управління та взаємовідносин всіх її елементів потребує і сфера підтримки інформаційної безпеки. Конституцією України ця сфера визначена як самостійний об'єкт державного управління, хоча вона є невід'ємною компонентою національної безпеки України.

II Сучасний стан функціонування системи інформаційної безпеки

Серед багатьох теоретичних проблем державного управління (філософських, економічних, кібернетичних, політичних) важливішими, на погляд автора, є розроблення та удосконалення організаційно-правових засад, оскільки саме на них ґрунтується процес здійснення державного управління. Створення владних структур, здійснення ними завдань та функцій ґрунтується на існуючих в суспільстві організаційно-правових засадах. Останні є "основою", "фундаментом" ефективності взаємовідносин органів державної влади при досягненні певних загальнодержавних, суспільно значущих цілей в будь-якій сфері державного управління.

Поняття взаємовідносин достатньо містке і складне. Отже, закономірним є різноманітність їх визначень. Частина фахівців трактує його як процес узгодження і взаємного урахування різних соціальних інтересів; друга – як взаємообумовлений процес впливу одних соціальних груп на інші, третя – як керований процес реалізації зв'язків, що будується на базі загального і специфічного в діяльності взаємодіючих суб'єктів з метою досягнення нового якісного рівня, четверта – як об'єднання зусиль сторін для вирішення того чи іншого питання, організації спільних дій [2].

Слід зазначити, що при дослідженні взаємовідносин органів державної влади в сфері інформаційної безпеки ще немає системності. Але це зовсім не свідчить про те, що зазначену проблему не вважають актуальною. Про налагодження плідних взаємовідносин між владними структурами, задіяними в механізмі забезпечення національної та інформаційної безпеки як її складової й про взаємодію між усіма суб'єктами її забезпечення згадувалося майже на всіх парламентських слуханнях Верховної Ради III скликання "Проблеми інформаційної діяльності, свободи слова, дотримання законності та стану інформаційної безпеки України", на багатьох семінарах та конференціях, присвячених цій проблематиці.

Однак, нагадування про налагодження тісних взаємин та доцільність взаємодії в сфері забезпечення інформаційної безпеки ще не є вирішенням проблеми.

Дослідження організаційно-правових питань удосконалення взаємовідносин органів державної влади в сфері інформаційної безпеки слід розпочати з визначення системи органів (суб'єктів) щодо підтримання інформаційної безпеки.

Загальну систему суб'єктів забезпечення інформаційної безпеки складають:

1) органи законодавчої влади і державного управління загальної компетенції – Верховна Рада України, Кабінет Міністрів України;
2) Конституційний суд, суди загальної юрисдикції;
3) органи виконавчої влади:
   а) правоохоронні органи – Прокуратура України, Міністерство внутрішніх справ України, Служба безпеки України;
   б) галузеві органи державного управління, що регулюють інформаційні відносини в певних галузях – Державний комітет зв'язку та інформатизації України, Державний комітет телебачення і радіомовлення України, Державний департамент інтелектуальної власності, Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України;

4) громадські структури – підприємства, установи, організації різних форм власності, діяльність яких пов'язана з наданням послуг зв'язку, із захистом інформації, інформаційні агентства, суб'єкти видавничої справи.

Координаційним органом з питань національної безпеки є Рада національної безпеки і оборони України, яка координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони. Головою Ради національної безпеки і оборони України відповідно до ст. 107 Конституції України є Президент України.

III Деякі організаційно-правові проблеми забезпечення інформаційної безпеки

Зазначена система завдяки взаємодії всіх гілок влади та громадських структур формально гарантує підтримання національної безпеки в державі. Але на практиці ми дуже часто зустрічаємося з відсутністю чіткої координації зусиль в сфері забезпечення інформаційної безпеки. Спостерігається такий собі ефект «лебідь, рак і щука», коли кожен елемент зазначеної системи або «тягне ковдру на себе», намагаючись отримати перевагу перед іншими, або дублює дії іншого.

Як приклад такого "ефекту" можна привести те, що в механізмі забезпечення інформаційної безпеки задіяно не один орган державної влади. В цьому механізмі приймають участь органи державного управління, що реалізують державну політику в інформаційній сфері в певних галузях та напрямках (Держкомзв'язку та інформатизації, Держкомінформполітики, СБУ, МО, МВС та ін.). Чи не цікавим є той факт, що розробкою Концепції забезпечення інформаційної безпеки займаються всі ці органи, але кожний окремо. Чи можна вести мову про єдину державну політику, єдину стратегію забезпечення інформаційної безпеки, коли кожен твердо відстоює свої позиції та вважає, що його сфера інформаційної діяльності є найважливішою та найвразливішою. Рішення Ради НБО безумовно є важливими, оскільки торкаються найгостріших проблем національної безпеки та оборони держави, однак приймаються вони в міру проведення засідань Ради.

З метою уникнення зазначеного відчувається реальна потреба в органі, що буде безпосередньо виконувати завдання забезпечення інформаційної безпеки, при чому зі статусом не дорадчим, а постійно діючим.

Практика створення Міжвідомчих робочих груп, на думку автора, себе не виправдовує. Про це свідчить діяльність структур, створених з метою врегулювання правових питань, визначення та організації реалізації державної політики в сфері інформаційних відносин, таких як Міжвідомчий комітет з проблем захисту прав на об'єкти інтелектуальної власності, Міжвідомча робоча група з розроблення та узгодження Концепції легалізації програмних продуктів та боротьби з нелегальним їх використанням. Розпорядженням №181-р від 06 травня 2001 року Уряду України створено міжвідомчу робочу групу для розробки проекту Концепції інформаційної безпеки та Програми боротьби зі злочинами в сфері інформаційних технологій. Однак, результативність діяльності цих структур характеризується введенням економічних санкцій США до нашої країни за неналежну боротьбу з порушеннями прав інтелектуальної власності, переважно щодо комп'ютерних програмних продуктів.

До того ж, наразі питання введення проти України економічних санкцій за неналежний рівень додержання та захисту авторських прав та ліцензійних умов при виготовленні і реалізації об'єктів інтелектуальної власності, надмірного рівня контрафактної продукції залишається актуальним.

На думку автора, проблема полягає в недостатній увазі до організаційно-правових засад забезпечення інформаційної безпеки. А звідси випливає й неналежний рівень організації та координації, пасивність органів державної влади щодо співробітництва, відсутність взаємодії при досягненні загальної мети.

Необхідно зазначити, що можуть існувати різні форми взаємодії державних органів між собою (в тому числі в сфері підтримання інформаційної безпеки):

- співробітництво – якщо партнери плідно співробітничають та активно сприяють один одному для досягнення спільної мети;
- протиборство – коли партнери протидіють один одному;
- ухилення від взаємодії;
- однонаправлена взаємодія – коли один з учасників ухиляється від взаємодії, а інший сприяє досягненню або цілей іншого, або спільних цілей;
- однонаправлене протиборство – коли один з партнерів протидіє досягненню цілей іншого, а другий ухиляється від взаємодії з першим;
- контрастна взаємодія – один з учасників намагається сприяти іншому, а другий використовує стратегію активної протидії стосовно першого;
- компромісна взаємодія – якщо партнери проявляють окремі елементи як сприяння, так і протидії [3].

Найбільш перспективним видом взаємодії є співробітництво, що дозволяє досягти реального, максимально можливого результату. Отже, реальне, а не формальне підтримання інформаційної безпеки, що

є кінцевою метою діяльності створеної системи органів державної влади, можливе лише при співробітництві цих органів.

Абсолютно очевидним є той факт, що дублювання діяльності окремих органів державної влади веде до безпідставного, невиправданого їх бюджетного фінансування, і це виступає суттєвим чинником, який має спонукати державні органи до активізації співробітництва.

Поява все більшої кількості загроз інформаційній безпеці країни і зокрема стрімке зростання "комп'ютерної злочинності" накладає відбиток на адміністративну діяльність існуючої системи органів державної влади в сфері інформаційної безпеки, змінюючи не тільки характер її основних, сформованих функцій, задач і напрямків діяльності, але і структуру.

В період інформатизації на органи державної влади, покликані підтримувати інформаційну безпеку, поряд із завданнями підтримання національної безпеки в цілому, покладаються нові, раніше не властиві їм завдання та функції – організація системи захисту інформації і діяльності з протидії "комп'ютерній злочинності". Така діяльність, з одного боку, виступає необхідною складовою процесу захисту інформації, з іншого боку – є одним з напрямків правоохоронної діяльності, що виконується відповідними державними органами в межах їхньої компетенції. Якщо першу з них також можна віднести до внутрішньої, властивої не тільки системі правоохоронних органів, то друга носить загально соціальний характер, тому що впливає на процеси управління інформатизацією суспільства в цілому [4].

IV Шляхи удосконалення системи забезпечення інформаційної безпеки

Поява таких специфічних, раніше не властивих державним органам функцій, спричиняє цілий ряд проблем комплексного характеру, які можна розв'язати шляхом глобального реформування, а також удосконалення їхньої діяльності, організації спеціальних структур, зміни кадрового складу і т. п. [5].

Тому виникає необхідність детального розгляду принаймні двох найважливіших проблем організації діяльності органів державної влади, в тому числі правоохоронних органів, і пов'язаних з ними практичних управлінських рішень. Мова йде про реалізацію конкретних заходів щодо створення системи, здатної скоординувати діяльність розглянутих органів державної влади, пов'язану з інформатизацією відомств і протидією негативним явищам у цій сфері.

В сфері захисту державних інформаційних ресурсів, на думку автора, цю проблему можна вирішити. По-перше, необхідно чітко розподілити та регламентувати функції щодо координації суб'єктів забезпечення інформаційної безпеки. При цьому роль «координатора» має бути посилена, а виконувати її має Рада національної безпеки і оборони України. Цим органом має бути вироблена чітка політика, що передбачає колегіально обговорені і закріплені документально позиції за основними напрямками адміністративної діяльності, пов'язаними із процесами інформатизації, захисту інформації, а також профілактики і боротьби з правопорушеннями, що вчинюються із застосуванням інформаційних технологій.

По-друге, окрім координуючого органу потрібен також "генератор" ідей – "виконавець", який буде здійснювати практичну координацію органів державної влади та інших суб'єктів загальнодержавної системи інформаційної безпеки в сфері захисту державних інформаційних ресурсів. Значним кроком до удосконалення забезпечення інформаційної безпеки буде створення в складі вже існуючого органу державної влади структурного підрозділу – Державного Центру безпеки інформаційних та телекомунікаційних мереж , який би безпосередньо виконував функції координації діяльності всіх суб'єктів забезпечення інформаційної безпеки в сфері захисту державних інформаційних ресурсів для виявлення, реагування та ліквідації наслідків несанкціонованих дій щодо державних інформаційних ресурсів у інформаційних та телекомунікаційних системах.

Наступним кроком в організації роботи правоохоронних органів мають стати практичні заходи щодо створення системи протидії комп'ютерним правопорушенням, а саме створення в органах державної влади спеціальних підрозділів захисту інформаційно-телекомунікаційних мереж протидії правопорушенням, вчиненим з використанням інформаційних технологій, а також розробка механізму їхньої координації. А для ефективної реалізації функцій та завдань Державного Центру необхідно розробити Порядок взаємодії між Державним Центром та цими підрозділами.

Вивчення закордонного досвіду і аналіз організаційно-правових основ діяльності спеціальних підрозділів захисту інформації та підрозділів по боротьбі з "комп'ютерними правопорушеннями" показав, що такі підрозділи існують практично в усіх цивілізованих країнах. Крім того, створення системи і механізму протидії такого роду злочинам є одним з головних вимог Ради Європи до країн, що бажають приєднатися до Європейського союзу. Про серйозність та важливість проблеми свідчать вражаючі офіційні статистичні дані Інституту комп'ютерної безпеки (Computer Security Institute). У 2000 році тільки в США економічні збитки від дій комп'ютерних злочинців склали 265,6 млн. доларів США. У Франції щорічні втрати банків досягають 1 млрд. франків на рік, кількість таких злочинів збільшується на 30–40 відсотків. У Німеччині від злочинів у

сфері використання комп'ютерних технологій збитки становлять близько 4 млрд. марок за рік. У Великій Британії лише асоціація страхових компаній несе збитки на суму понад 1 млрд. фунтів стерлінгів на рік.

Окрім того, протидія злочинам, що скоєні з використанням інформаційних технологій, має здійснюватися спеціальними підрозділами, створеними в усіх правоохоронних органах і діючих комплексно і скоординовано в рамках їхньої компетенції.

Вражає кількість думок та теоретичних досліджень, що стосується оптимізації системи забезпечення інформаційної безпеки, створення ефективної моделі взаємовідносин органів державної влади в зазначеній сфері. Одна група вчених пропонує провадження координації суб'єктів забезпечення інформаційної безпеки громадською організацією – Асоціацією захисників інформації, інші фахівці пропонують створити Координаційну Раду з питань політики інформатизації правоохоронних органів, або створити в державі центральний орган державної виконавчої влади, який наділити відповідними повноваженнями. Зазначені думки безперечно заслуговують на увагу, однак їх реалізація ставить під сумнів подальше функціонування існуючих органів держави, на яких покладено забезпечення інформаційної безпеки держави.

V Висновки

Аналіз наукових публікацій, що теоретично обґрунтовують доцільність створення органу, який зможе скоординувати всі суб'єкти забезпечення інформаційної безпеки та сконцентрувати їх зусилля в певних напрямках її підтримання, свідчить про те, що їх автори, відстоюючи інтереси певних державних та недержавних структур, не враховують, що в загальнодержавній системі забезпечення інформаційної безпеки існують органи, які вже створені з цією метою.

Враховуючи стан інформаційних та телекомунікаційних мереж органів державної влади, вразливість до несанкціонованого доступу, змін (знищення) інформації, що в них циркулює, вірусного ураження тощо сьогодення вимагає створення Державного Центру безпеки інформаційних та телекомунікаційних систем, причому не з окремим статусом, а зі статусом структурного підрозділу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, оскільки згідно з Положенням про ДСТСЗІ СБ України, затвердженим Указом Президента № 1120 від 06. 10. 2000 року, саме Департамент, реалізує державну політику у сфері захисту державних інформаційних ресурсів.

Створення Державного центру безпеки інформаційних та телекомунікаційних систем при Департаменті є позитивним моментом в сучасному процесі забезпечення національної безпеки. Серед проблем (фінансово-економічних, матеріально-технічних, кадрових та ін.), що підлягатимуть вирішенню в ході його діяльності, безумовно будуть проблеми налагодження ефективних взаємовідносин з органами державної влади та іншими суб'єктами системи забезпечення інформаційної безпеки. Саме в удосконаленні вже існуючих та в налагодженні нових взаємин залежить плідне та ефективне функціонування Державного Центру безпеки інформаційних та телекомунікаційних систем. Тобто, наступним кроком за створенням умов для належного функціонування Державного Центру безпеки має стати розробка шляхів взаємодії з іншими суб'єктами системи забезпечення інформаційної безпеки, механізму їхньої координації.

Одним з перспективних завдань, що стосується удосконалення взаємовідносин, окрім укладення міжнародних Угод про співробітництво, буде розробка певного порядку взаємодії з підрозділами інших правоохоронних органів і міжнародних структур, що мають аналогічні задачі. Це надасть можливість вивчити досвід правоохоронних органів інших країн щодо виявлення порушень, реагування на них, ліквідації наслідків несанкціонованих дій в інформаційно-телекомунікаційних мережах та профілактики комп'ютерним правопорушенням.

На законодавчому рівні, думається, необхідним є прийняття програмного документу (Державної програми), який окреслить основні принципи, концепції, доктрини, що визначають політику держави в такій галузі інформаційних відносин, як виявлення, реагування та ліквідація наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних та телекомунікаційних системах і профілактики комп'ютерним правопорушенням. Окремим розділом необхідно передбачити можливі форми та принципи взаємодії та відповідно до Державної програми розробити міжвідомчі інструкції, положення, що будуть розкривати зміст взаємовідносин та процедуру взаємодії між суб'єктами системи (з урахуванням специфіки діяльності кожного з них в певних напрямках функціонування).

Окрім того, враховуючи те, що інформаційна безпека є комплексною проблемою, мінімізація її проявів потребує застосування сучасних наукових методів (математичних, кібернетичних тощо) і дослідження організаційно-правових аспектів, саме зі змісту яких в значній мірі випливає та залежить досягнення поставлених державою завдань та цілей.

Література : 1. О. Цвєтков «Ефективність державного управління: організаційно-правові аспекти, К. 1998. 2. О. Комаровский. Связи с общественностью в политике и государственном управлении. – М., 2001. –

с. 254. 3. Беляков К. Управление и право в период информатизации. – К.: КВІЦ, 2001. – 292, 294, 295. 4. Інформаційне право та інформаціна безпека / Сучасний стан, поняття та визначення змістовної частини, інкорпорація нормативних актів з правових питань у сфері інформації та її захисту / заг. Ред. Р. Калюжного та В. Філонова – Київ-Донецьк: Донецький інститут внутрішніх спарав МВС України. Інститут економіки та права «Крок», 2001. – 230 с. 5. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп»ютерних тезхнологій. Монографія / За заг. ред. д. ю. н. Калюжного Р. А. – Запоріжжя 6 «Просвіта», 2001. – 252 с.