КООРДИНАЦІЙНИЙ КОМІТЕТ
ПО БОРОТЬБІ З КОРУПЦІЄЮ І ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ
ПРИ ПРЕЗИДЕНТОВІ УКРАЇНИ

МІЖВІДОМЧИЙ НАУКОВО-ДОСЛІДНИЙ ЦЕНТР
З ПРОБЛЕМ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ

Проект

КОНЦЕПЦІЯ

СТРАТЕГІЇ І ТАКТИКИ
БОРОТЬБИ З КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ
В УКРАЇНІ

Київ -2001

ПРОЕКТ КОНЦЕПЦІЇ СТРАТЕГІЇ І ТАКТИКИ БОРОТЬБИ З КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ В УКРАЇНІ РОЗРОБЛЕНИЙ ЗА ІНІЦІАТИВОЮ ГУБОЗ МВС УКРАЇНИ ВІДПОВІДНО ДО ПЛАНУ НАУКОВО-ДОСЛІДНИХ РОБІТ МІЖВІДОМЧОГО НАУКОВО-ДОСЛІДНОГО ЦЕНТРУ З ПРОБЛЕМ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ НА 2001 РІК, ЗАТВЕРДЖЕНОГО ГОЛОВОЮ КООРДИНАЦІЙНОГО КОМІТЕТУ ПО БОРОТЬБІ З КОРУПЦІЄЮ І ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ ПРИ ПРЕЗИДЕНТОВІ УКРАЇНИ

Проект

КОНЦЕПЦІЯ СТРАТЕГІЇ І ТАКТИКИ БОРОТЬБИ З КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ В УКРАЇНІ

Однією з відмінних, визначних ознак сучасного світового соціального прогресу є зростання значимості інформації в суспільних відносинах.

Суспільні інформаційні відносини постійно розвиваються, особливо з удосконаленням техніки та технологій збирання, обробки, зберігання та передавання інформації. Зазначені процеси визначають сутність інформаційного суспільства.

Поряд із позитивними здобутками в інформаційному суспільстві виникли соціальні проблеми криміногенного характеру, які потребують вирішення на державному рівні:

організація інформаційної безпеки людини, соціальних спільнот, держави як важливих провідних напрямів національної безпеки України та інших її складових, у тому числі економічної безпеки;

мінімізація наслідків соціогенних загроз особі, суспільству, державі, у тому числі, криміногенних, зокрема, злочинів, що вчиняються з використанням комп'ютерних інформаційних технологій, через електронні засоби телекомунікації;

забезпечення права власності на інформацію (інформаційних прав) людини, суспільних формувань, держави як вид майна, що перебуває у суспільному обігу не менше рівня права власності на речі (речових прав);

формування засад державної політики щодо організації протидії іншим негативним проявам інформаційного суспільства.

Зазначені проблеми зумовили необхідність розробки концепції стратегії і тактики боротьби з комп'ютерною злочинністю (кіберзлочинністю) в Україні.

Особливу небезпеку для держави і суспільства має прояв кіберзлочинності з ознаками організованої.

Частина 1. Загальні положення

Основні напрями стратегії і тактики боротьби з комп'ютерною злочинністю розвивають основні положення, принципи, концепції, доктрини, що визначають політику держави у сфері суспільних інформаційних відносин.

Концепція стратегії і тактики боротьби з комп'ютерною злочинністю в Україні (далі Концепція), як нормативно-правовий акт, визначає основні, найважливіші засади державної політики, організації та управління органами державної влади щодо профілактики, попередження, виявлення та розкриття злочинів, які вчиняються з використанням комп'ютерних інформаційних технологій, а також виявлення причин та умов вчинення таких злочинів, комп'ютерної злочинності в цілому з метою зменшення їх негативного впливу на окремих громадян, інших людей, які перебувають на законних підставах в Україні, громадські організації, суспільство, державу.

Ця Концепція також визначає основні засади напрямів міжнародного співробітництва України з іншими державами щодо протидії транскордонній кіберзлочинності.

Розділ 1. Визначення основних понять та категорій

За Концепцією окремі провідні поняття та категорії визначаються у наступному змісті:

Інформаційна цивілізація – історично визначені, на геополітичному рівні, соціальні стандарти розвитку глобального суспільства (Земної цивілізації), що характеризуються діяльністю людей, яка здійснюється на основі послуг, які надаються за допомогою комп'ютерної техніки та

електронних інформаційних технологій, у тому числі електронного зв'язку, тобто телекомунікацій через проводові (дротяні), радіо-релейні та штучні космічні супутникові технології передавання та отримання інформації.

Інформаційне суспільство – суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою електронних інформаційних технологій та технологій зв'язку.

Інформаційне середовище суспільних відносин – комплекс відповідним чином упорядкованих технічних та технологічних засобів, автоматизованих (комп'ютерних) систем обробки інформації, телекомунікаційної інфраструктури та інтелекту суб'єктів, які здійснюють збирання, формування, розповсюдження та використання інформації, а також системи правовідносин щодо інформації, що виникають в процесі суспільної діяльності.

Інформаційна безпека – вид інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов їх життєдіяльності; суспільні процеси, пов'язані зі створенням безпечних (нормальних) умов поширення, розповсюдження, зберігання та використання інформації; стан правовідносин пов'язаний з нормальним (безпечним) створенням, розповсюдженням, обробкою зберіганням та використанням інформації у певному просторі, часі та колі осіб.

Комп'ютерна інформація (інформація в автоматизованих (комп'ютерних) системах) – відповідним чином упорядкована інформація (дані і комп'ютерні програми), що існує або циркулює в комп'ютерних автоматизованих системах чи мережах незалежно від засобу (способу, методу) їх фізичного та логічного подання (представлення).

Комп'ютерна злочинність (кіберзлочинність) – історично зумовлене антисоціальне явище інформаційного суспільства, яке охоплює всю множину комп'ютерних злочинів, вчинених особами в Україні, чи з України, чи щодо

об’єктів злочинного посягання в Україні особами, які перебувають за її межами у визначеному проміжку часу.

Комп’ютерний злочин (кіберзлочин) – суспільно-небезпечні дії, які передбачені кримінальним законодавством України як злочин, що вчинений з використанням комп’ютерних продуктів або у якому комп’ютерні продукти є предметом чи засобом злочинного посягання; злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж.

Комп’ютерні продукти – відповідним чином упорядкована множина інформації (відомостей, даних, знань), що призначена для обробки або обробляється в автоматизованих (комп’ютерних) системах, а також комп’ютерні програми, автоматизовані (комп’ютерні) бази даних, автоматизовані (комп’ютерні) бази знань, топографії (топології) інтегральних мікросхем, інші форми інформації, що обробляється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих комп’ютерних системах чи циркулює у відповідних електронних мережах телекомунікації.

Визначення змісту складових комп’ютерних продуктів здійснюється відповідно до чинного інформаційного законодавства України, а також авторського права та похідних від нього інших видів права інтелектуальної власності.

Протидія комп’ютерній злочинності (боротьба з комп’ютерною злочинністю) – діяльність суб’єктів суспільних відносин відповідно до законодавства України щодо:

виявлення, упередження (профілактики), розкриття, розслідування комп’ютерних злочинів та притягнення винних до відповідальності;

виявлення та усунення технічних загроз інформаційній безпеці людини, суспільству, державі, які можуть використовуватися для вчинення правопорушень;

виявлення причин і умов вчинення злочинів та мінімізація їх наслідків.

Організація протидії комп'ютерним правопорушенням здійснюється відповідно до положень адміністративного, цивільного, трудового та кримінального законодавства, а також інформаційного та інших підгалузей законодавства.

Суспільні інформаційні відносини (інформаційні правовідносини) – суспільні відносини щодо інформації; суспільні відносини об'єктом яких є інформація; суспільні відносини щодо одержання, використання, поширення та зберігання інформації (відомостей, даних, знань) у всіх сферах життя і діяльності особи, суспільства і держави; суспільні відносини, які виникають, здійснюються та припиняються в процесі інформаційної діяльності.

Особа – фізична (приватна) або юридична особа. Ознаки особи визначаються відповідно до чинного цивільного та адміністративного законодавства України, а також практики міжнародного права, його складових – міжнародного публічного та міжнародного приватного права.

Розділ 2. Система правового регулювання суспільних інформаційних відносин в умовах інформатизації України (інформаційного суспільства)

Система правового регулювання суспільних інформаційних відносин в умовах інформатизації (інформаційного суспільства) України базується на доктрині поділу права на публічне (державне) і приватне.

Публічне (державне) регулювання суспільних інформаційних відносин знаходить вираз у системі законодавства та підзаконних нормативних актах, виданих відповідно до компетенції Президентом України, Кабінетом Міністрів України, органами державної виконавчої і судової влади та органами місцевого самоврядування.

Провідними принципами публічного права у сфері діяльності органів державної влади щодо суспільних відносин в основі яких є інформація наступні:

юридичне закріплення прав, обов'язків, зобов'язань, гарантій та відповідальності державних органів влади перед особами і суспільством;

визначення та забезпечення співвідношення інтересів людини, суспільства, держави у сфері суспільних інформаційних відносин;

законність.

Приватне правове регулювання суспільних інформаційних відносин в Україні здійснюється приватними особами (фізичними і недержавними юридичними особами, громадськими формуваннями) на засадах:

норм публічного правового регулювання з урахуванням законних прав та інтересів інших осіб і суспільства;

конституційного принципу дозволеності діянь, не заборонених законодавством;

автономії волі приватних осіб щодо виникнення, здійснення та припинення правовідносин (через правочини, угоди (статути), добрі звичаї, норми суспільної моралі, корпоративної (ділової) етики тощо).

Правове регулювання протидії кіберзлочинам та кіберзлочинності базується на засадах інформаційного законодавства, яке є комплексною галуззю законодавства України.

Основу публічно-правового регулювання суспільних інформаційних відносин становить Конституція України.

Розвиток положень Конституції України щодо регулювання суспільних інформаційних відносин відображені в окремих нормах кодифікованих провідних галузей законодавства:

Кримінальний кодекс України;

Кримінально-процесуальний кодекс України.

Цивільний кодекс України;

Цивільний процесуальний кодекс України;

Кодекс України про адміністративні правопорушення;

Кодекс законів про працю України.

Окремі норми суспільних інформаційних відносин містяться в:

Митному кодексі України;

Арбітражному процесуальному кодексі України;

інших кодексах України;

Основах законодавства України щодо окремих галузей суспільних відносин.

2.1. Законодавство у сфері боротьби з комп'ютерною злочинністю

Спеціальне законодавство щодо боротьби з комп'ютерною злочинністю ґрунтується на законодавстві провідних галузей права, у тому числі у сфері правоохоронної діяльності, і складається із законів, що визначають компетенції та функцій окремих державних органів влади: прокуратури, міліції, служби безпеки, державної податкової служби. Також окремі положення боротьби з комп'ютерною злочинністю визначені у законодавстві України про оперативно-розшукову діяльність, про організаційно-правові основи боротьби з організованою злочинністю, про боротьбу з корупцією, про оборону, про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності, про захист від недобросовісної конкуренції, інших законодавчих актах, в яких визначається компетенція, функції суб'єктів суспільних інформаційних відносин.

2.2. Спеціальне законодавство у сфері суспільних інформаційних відносин в Україні

Протидія кіберзлочинам та кіберзлочинності в Україні грунтується на нормах спеціального інформаційного законодавства, основу якого становить Закон України "Про інформацію".

Положення цього Закону знаходять свій розвиток в законодавчих нормах, які є системоутворювальними щодо публічно-правового (державного) регулювання **окремих сфер суспільних інформаційних відносин,** у тому числі Законах України: про мови; про державну таємницю; про авторське право і суміжні права; про науково-технічну інформацію; про бібліотеки і бібліотечну справу; про Національний архівний фонд і архівні установи; про

обов'язковий примірник документів; про розповсюдження примірників аудіовізуальних творів та фонограм тощо.

Умовно-автономний субінститут інформаційного законодавства утворює **законодавство у сфері зв'язку та інформатизації**, яке складається із системоутворювальних Законів України: про зв'язок, про захист інформації в автоматизованих системах; про Концепцію Національної програми інформатизації; про Національну програму інформатизації; про охорону прав на топографії інтегральних мікросхем.

2.3. Інші законодавчі акти України, які регулюють суспільні інформаційні відносини

Автономні субінститути інформаційного законодавства утворюють Закони України **у сфері масової інформації**: про друковані засоби масової інформації (пресу) в Україні; про інформаційні агентства; про видавничу справу; про телебачення і радіомовлення; про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації; про систему суспільного телебачення і радіомовлення; про національну раду України з питань телебачення і радіомовлення; про радіочастотний ресурс України; про кінематографію, інші законодавчі акти.

2.4. Міжгалузевий зв'язок інформаційного законодавства

Як опосередкований об'єкт, інформація виступає з'єднувальною ланкою з іншими міжгалузевими інститутами законодавства.

До провідних системоутворювальних законодавчих актів, які містять норми суспільних відносин, виражені через інформацію, належать Закони України про власність, про рекламу, державну статистику, бухгалтерський облік та фінансову звітність в Україні, охорону культурної спадщини, освіту, загальну середню освіту, професійно-технічну освіту, наукову і науково-технічну діяльність, наукову і науково-технічну експертизу, метрологію та

метрологічну діяльність, топографо-геодезичну і картографічну діяльність, гідрометеорологічну діяльність, застосування електронних контрольно-касових апаратів і товарно-касових книг при розрахунках із споживачами у сфері торгівлі, громадського харчування та послуг, Державний реєстр фізичних осіб - платників податків та інших обов'язкових платежів, Національну депозитарну систему та особливості електронного обігу цінних паперів в Україні, інші законодавчі акти.

Інформація, як один з важливих чинників, виступає у сфері економічних правовідносин (банківських, господарських, комерційних, підприємницьких, інвестиційних, іноваційних тощо), і знаходить своє відображення у системоутворювальному законодавстві - Законах України про банки і банківську діяльність, про економічну самостійність України; про зовнішньоекономічну діяльність; про підприємництво; про цінні папери і фондову біржу; про інвестиційну діяльність; про товарну біржу; про аудиторську діяльність; про регулювання товарообмінних (бартерних) операцій у галузі зовнішньоекономічної діяльності; про захист національного товаровиробника від демпінгового імпорту; про захист національного товаровиробника від субсидованого імпорту; про застосування спеціальних заходів щодо імпорту в Україну тощо.

Окремі положення щодо регулювання інформаційних правовідносин в умовах становлення в Україні інформаційного суспільства знайшли закріплення і відображення **в Постановах Верховної Ради України** про затвердження Концепції (основ державної політики) національної безпеки України; про організацію роботи по формуванню єдиної системи правової інформації в Україні; про Консультативну раду з питань інформатизації при Верховній Раді України та Положення про Консультативну раду з питань інформатизації при Верховній Раді України, в інших нормативно-правових актах Верховної Ради України.

Суспільні інформаційні відносини, як опосередкований об’єкт, регулюються також **Декретами Кабінету Міністрів України** про державний нагляд за додержанням стандартів, норм і правил та відповідальності за їх порушення; про стандартизацію і сертифікацію тощо.

2.5. Система підзаконних нормативно-правових актів щодо боротьби з комп’ютерною злочинністю в Україні

Державна політика України щодо боротьби з комп’ютерною злочинністю та комп’ютерними злочинами знаходить вираз у системі підзаконних нормативно-правових актів органів державної влади щодо їх компетенції. Її складають Укази Президента України, нормативно-правові акти Уряду України, нормативні акти міністерств і відомств щодо їх компетенції, функцій, прав і обов’язків.

Розвиток положень чинного законодавства знаходить відображення у конкретних підзаконних нормативно-правових актах, як:

Укази Президента України: про рішення Ради національної безпеки і оборони від 17 червня 1997 року “Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин”; про Комісію з питань інформаційної безпеки; про деякі заходи щодо захисту інтересів держави в інформаційній сфері; про єдину комп'ютерну інформаційну мережу державних органів приватизації; про електронний обіг цінних паперів і національний депозитарій; про Міжвідомчу комісію з питань приєднання України до Генеральної угоди з тарифів і торгівлі та вступу до Світової організації торгівлі; про Положення про Державний центр страхового фонду документації України; про заходи щодо впровадження Концепції адміністративної реформи в Україні; про державну реєстрацію нормативних актів міністерств та інших органів державної виконавчої влади; про Положення про державних експертів з питань таємниць, про Положення про технічний захист інформації в Україні; про заходи щодо розвитку

національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні; про заходи щодо захисту інформаційних ресурсів держави; про заходи щодо вдосконалення криптографічного захисту інформації в телекомунікаційних та інформаційних системах; про вдосконалення порядку здійснення організаційно-структурних змін у сфері забезпечення інформаційної безпеки; про Положення про порядок здійснення криптографічного захисту інформації в Україні; про Єдиний державний реєстр нормативних актів;

Постанови Кабінету Міністрів України: про першочергові заходи інформатизації; про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних; про затвердження плану заходів щодо формування інформаційно-аналітичної системи органів державної влади; про заходи щодо посилення контролю за обгрунтованістю проектів інформатизації діяльності центральних органів виконавчої влади; про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах; про уточнення термінів впровадження засобів контролю; про перелік відомостей, що не становлять комерційної таємниці; про Положення про порядок видачі суб'єктам підприємницької діяльності спеціальних дозволів (ліцензій) на здійснення окремих видів діяльності, про Порядок надання Кабінетом Міністрів України дозволу на використання запатентованого винаходу (корисної моделі) чи запатентованого зразка без дозволу власника патенту, але з виплатою йому відповідної компенсації; про Положення про технічний захист інформації в Україні; про створення Єдиного державного реєстру підприємств і організацій України; про Єдиний ліцензійний реєстр; про впровадження штрихового кодування товарів; про затвердження Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави; про утворення Міжвідомчого комітету з проблем захисту прав на

об’єкти інтелектуальної власності; про перелік платних послуг, які можуть надавати інформаційні підрозділи органів внутрішніх справ; про деякі питання реалізації державної інформаційної політики; про підписання Угоди між Кабінетом Міністрів України і Урядом Киргизької Республіки про співробітництво в галузі інформації; про створення єдиної комп’ютерної мережі арбітражних судів; про затвердження Положення про державну реєстрацію нормативних актів міністерств та інших органів державної влади; про затвердження Єдиного державного реєстру нормативних актів та здійснення правової інформатизації України; про державне підприємство “Інформаційний центр” Міністерства юстиції; про затвердження Генерального державного замовника Національної програми інформатизації; про керівника Національної програми інформатизації; про затвердження Положення про формування та виконання Національної програми інформатизації; про утворення експертно-консультативної ради з питань інформатизації при Кабінеті Міністрів України; про затвердження Порядку локалізації програмних продуктів (програмних засобів) для виконання Національної програми інформатизації; про Програму створення Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій; про заходи щодо створення єдиної бази статистичних даних та статистичної звітності про зовнішньоторговельні операції, інші нормативні акти Уряду України.

Розділ 3. Загальна характеристика комп’ютерної злочинності

3.1.Кримінологічні аспекти комп’ютерної злочинності

Правоохоронними органами України спільно з іншими державними та недержавними структурами починаючи з другій половини 90-х років виявляється і попереджується традиційними методами низка злочинів, які вчиняються за допомогою комп’ютерної техніки, у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж.

Найпоширеніші за способом вчинення є такі комп`ютерні злочини, як н**есанкціонований доступ до інформації в автоматизованих (комп'ютерних) системах.** Поширення сучасних електронних засобів та простота їх управлінням породжує потенційні загрози подолання технічного захисту інформації в автоматизованих (комп'ютерних) системах, у тому числі таких, що складають мережі телекомунікацій (окремих підприємств, галузевих, загальнодержавних, транскордонних). Це зумовлює потенційну об'єктивну і суб'єктивну недостатність технічної захищеності таких систем від несанкціонованого доступу, що становить соціогенну (зокрема криміногенну) загрозу. Крім того, виникають обставини, які зумовлюють ланцюгову реакцію щодо небажаного для конкретного суб'єкта суспільних інформаційних відносин несанкціонованого витоку інформації, її блокування (несанкціонованого обмеження доступу для правомірних користувачів інформації), спотворення (несанкціонованої модифікації) чи знищення інформації у комп'ютерній формі (комп'ютерної інформації).

3.1.1. Види комп'ютерних злочинів у галузях економіки

Для України найбільш відомими і характерними є комп'ютерні злочини у галузі економіки. Зафіксовані непоодинокі випадки вчинення правопорушень **у сфері кредитно-банківської системи**, коли зловмисники здійснювали спроби формування фіктивних електронних платежів з метою отримання незаконним шляхом коштів у регіональних відділеннях банків України.

Також зафіксовані спроби **несанкціонованого доступу до комп'ютерної мережі банків шляхом втручання в їх роботу і вчинення шахрайства, зловживання службовим становищем, службове підроблення документів.**

Нерідко, не маючи реальної наявності коштів на кореспондентських і субкореспондентських рахунках, при мінімальних кредитних залишках на кореспондентських рахунках, до проведення за дебетом подаються у електронному вигляді розрахунково-платіжні документи на значні загальні суми, чим допускається **несанкціонована емісія грошових коштів**.

Виявлено низку спроб **використання банківсько-кредитних технологій** та комп'ютерних інформаційних технологій для незаконного переведення через електронну систему платежів з використанням рахунків у Національному банку України до комерційних банків в Україні та за кордон.

Встановлено факти втручань в електронну банківську систему з метою **крадіжки грошей із застосуванням електронних платежів, у тому числі за допомогою пластикових кредитних та дебіторських карток**.

За роки існування системи електронних платежів, яка розроблена Національним банком України, неодноразово робились **спроби злому** її – несанкціонованого проникнення через подолання комп'ютерних систем технічного захисту за допомогою комп'ютерних програм. Правоохоронними органами спільно з управлінням захисту інформації Департаменту інформатизації Національного банку України та іншими його структурами виявлено та ліквідовано більше ніж 30 організованих злочинних угруповань, які спеціалізувалися на крадіжках грошей у банківській сфері.

Правоохоронні органи України неодноразово припиняли діяльність груп, які займалися **незаконною конвертацією безготівкових коштів в готівку іноземною валютою, у тому числі з використанням офшорних компаній.**

До валютних операцій залучені українські та іноземні фірми, здебільшого офшорні компанії, зареєстровані на підставних осіб. За допомогою комп'ютерних технологій зловмисники перераховують безготівкові кошти через українські банки на рахунки підставних фірм. Після цього гроші переводяться у валюту-готівку. Частина цих коштів повертається в Україну, а частина залишається за кордоном. Як правило, злочинні організації такого виду досить розгалужені регіонально.

3.1.2. Крадіжки комп'ютерної інформації та її знищення

За допомогою **несанкціонованого отримання паролів доступу** та інших засобів ідентифікації законних користувачів до захищених технічними засобами комп'ютерних систем у мережі Інтернет робляться спроби отримати

доступ до комп’ютерних інформаційних баз, переважно державних відомств з метою крадіжки інформації шляхом її копіювання, або знищення.

Мають місце випадки, коли правопорушники проникають до приміщень обчислювальних центрів комерційних та державних установ з метою викрадення (зняття копії) інформації та технологій її обробки. Нерідко викрадають не всю комп’ютерну техніку у потерпілих організаціях, а вилучають з комп’ютерів “вінчестери“ чи дискети, на яких міститься комп’ютерна інформація.

3.1.3. Порушення права інтелектуальної власності на комп’ютерні продукти (“комп’ютерне корсарство”, "комп’ютерне піратство", “інтелектуальне електронне корсарство”)

Порушення авторських прав та права інтелектуальної власності щодо володіння, розпорядження та користування комп’ютерними програмними продуктами. За даними Союзу боротьби з розкраданнями програмного продукту (Business Software Alliance (BSA), Україна визнана неконтрольованою територією, де 95% комп’ютерних програм експлуатуються без дозволу законних власників.

За даними міжнародних організацій, Україна в результаті “комп’ютерного корсарства” щорічно несе збитки близько 30 мільйонів американських доларів через несплату податків.

Високий рівень “інтелектуального електронного корсарства” є серйозною перешкодою для вступу України до Світової організації торгівлі, європейських структур, міждержавних регіональних економічних організацій та двосторонніх міждержавних економічних відносин.

3.2. Організована комп`ютерна злочинність

Комп’ютерна злочинність тісно пов’язана з різними видами організованої злочинності та корупції. Зокрема, “відмивання” грошей - зі злочинами у сфері застосування комп’ютерних технологій, що є частково непомітним виміром організованої злочинності.

За експертними оцінками на міжнародному рівні щорічно в світі “відмивається” 300-500 мільярдів доларів (з яких 30-40% походять від наркотиків, а решта як прибуот від фіскальних порушень, контрабанди зброєю, тероризму, шахрайства).

Організована кіберзлочинність посідає провідне місце поряд з наркобізнесом та торгівлею зброєю.

3.3. Види комп’ютерної злочинності за територіальними ознаками

Комп’ютерну злочинність за територіальними ознаками умовно поділяють на:

національну - в межах державних кордонів України;

транскордонну (транснаціональна, міжнародна):

глобальну – без обмежень у просторі і часі, у тому числі у всесвітніх мережах комп’ютерної телекомунікації,

континентальну – у межах окремих континентів,

регіональну (локальну) - між окремими країнами чи групами країн.

3.4. Організована транскордонна комп`ютерна злочинність з використанням Інтернет

Розвиток глобальних систем телекомунікації сприяє розвитку такого економічного явища, як електронної торгівлі (**е-комерція**). Не знаходиться поза цим процесом і Україна. Домінуюче місце в цьому явищі займає розвиток систем міжнародних валютних розрахунків за допомогою пластикових розрахункових карток, на зразок VISA. Організовані транскордонні злочинні формування також активно “освоюють” цей сегмент економічних відносин для організації злочинного бізнесу: підробки розрахункових пластикових карток, шахрайства з банкоматами тощо.

Нелегальні конвертаційні центри використовуються злочинними формуваннями для проведення протизаконних валютних операцій із застосуванням мережі Інтернет, у тому числі надання послуг іншим суб’єктам

господарської діяльності для ухилення від сплати податків, конвертації валют тощо.

Порушення авторських прав та права інтелектуальної власності на комп'ютерні програмні продукти (організоване «комп'ютерне піратство»). Дослідження, що проводяться протягом багатьох років у 70 країнах світу на замовлення Асоціації виробників комп'ютерних програм (BSA) і Асоціації видавців комп'ютерних програм (SPA) Міжнародною корпорацією планування і дослідження, свідчать, що з 523 млн нових прикладних комп'ютерних програм ділового призначення 225 млн одиниць (майже кожна друга) - неліцензійна копія.

На міжнародному рівні Україна віднесена до країн, де найвищий рівень порушення таких прав.

Нелегальна індустрія комп'ютерних програмних продуктів в Україні, за експертними оцінками, має рівень регіону Східної Європи з найвищим показником, зокрема щодо комп'ютерних програм (в середньому – майже 80%).

Дані про ринок нелегального комп'ютерного програмного забезпечення експерти наводять у порівнянні з іншими країнами: Країни Східної Європи, як і країни третього світу, в колі лідерів: Словенія - 96%; Болгарія - 94%; Румунія - 93%; Росія - 90%; Чехія - 62%; Словаччина - 62%; Україна - 90 %. Щорічні збитки розробників комп'ютерних програм становлять приблизно 750 млн доларів США.

Щодо таких країн, як Україна, організоване комп'ютерне піратство призводить до руйнування національної індустрії комп'ютерних програмних продуктів, знецінення престижу фахівців - виробників комп'ютерних програмних продуктів, зменшення їх рівня матеріального забезпечення, розвитку тіньової економіки у сфері виробництва комп'ютерних програмних продуктів, ухилення від сплати податків, відтік висококваліфікованих кадрів у сфері комп'ютерної індустрії за кордон.

3.5. Хакерський рух, як соціальне явище і як база організованої злочинності

Значного поширення з розвитком глобалізації інформатизації суспільства набуває таке соціальне явище, як хакерський рух – формування корпорацій осіб одержимих знаннями до комп'ютерних технологій. Зафіксовані непоодинокі випадки коли організовані злочинні формування використовують учасників цього руху для вчинення комп'ютерних злочинів. За експертними оцінками хакерський рух, окремі його представники є базою для комп'ютерної злочинності.

Хакери (одержимі комп'ютерні програмісти) проводять міжнародні, у тому числі всесвітні, зльоти, з'їзди (Ізраїль, Росія та інші країни). Мета хакерського руху - показати справжнє обличчя хакера: "Вони не ті люди, які зламують комп`ютери. Ті, хто це робить, - крекери... Хакери - це ті люди, які трудяться для того, щоб інші робили комп'ютерні програми краще". Як свідчать дослідження, межі між хакером незловмисником і крекером (хакером зловмисником) знайти майже неможливо. Нерідко "хакери – одинаки" чи їх спільноти, не розуміючи своєї ролі, виконують замовлення кримінальних угруповань.

За оцінками зарубіжних спеціалістів, лише на території США функціонують десятки тисяч хакерських BBS, з яких від 100 до 200 - спеціалізовані BBS (для фанатів-хакерів), а приблизно 1000 - є джерелом важливої інформації для широкого кола хакерів (зокрема, про доступні засоби комп'ютерного зламу різних систем, комп'ютерне програмне забезпечення для перехоплення паролів тощо).

Хакерські спільноти можуть групуватися за національними ознаками та залежно від кордонів територій держав. У світі, наприклад, відомі асоціації хакерів Великобританії, Італії, інших країн Східної Європи. Це знаходить відображення на відповідних "сайтах" у мережі Інтернет, де здійснюється концентрація хакерських BBS. При цьому такі "сайти", "веб-сторінки" не обов'язково можуть бути розміщені у країні - належності спільноти. Вони, як правило, розміщуються у країнах операторів Інтернет, де низький рівень

боротьби з ними як на державному рівні, так і серед законослухняної “кібергромадськості”.

Хакери мають власні електронні та друковані видання. Існує версія, що такі видання (особливо друковані) фінансуються як окремими хакерами, які заробляють великі гроші на злочинному бізнесі, так і різними терористичними організаціями, як форма залучення простаків (“хакерів-чайників”) до безпорядків у кіберпросторі (рекрутів до кіберхаосу).

Визначити масштаби проблеми, пов’язаної з діяльністю хакерських спільнот, дуже складно. Перш за все, це пояснюється невеликою кількістю відомих для правоохоронних органів фактів. Друге - більшість громадськості здебільшого терпляче (поки що) ставляться до правопорушень хакерів, не розуміючи, що комп’ютерні системи залишаються дуже вразливими для хакерів і будуть такими завжди. Пошкодити кабель зв’язку і несанкціоновано приєднатися до комп’ютерної мережі, вгадати пароль входу до комп’ютера, змінити атрибути файлів у автоматизованій базі даних, стерти зашифрований файл, замінити числа у бухгалтерській звітності - все це досить просто для хакера, які б досконалі технічні та програмні замки не створювали винахідники. Девіз хакерів: “Що створено руками одних, з часом буде зламано руками інших, особливо якщо за це взятися громадою”.

За оцінками експертів, загальна кількість атак хакерів на комп’ютерні робочі місця постійно зростає. Наприклад, за повідомленнями із США, їх кількість зросла з 339000 у 1989 році, до 423000 у 1990 році. У 1991 році цей показник налічував вже 684000 випадків. З початку 1991 року відлік йде за іншими критеріями: кількість хакерських атак сягнула близько 1,6 (у тому числі повторних) на 100 комп’ютерів за рік.

Загальні втрати від атак хакерів обчислювалися експертами у 81,6 мільйонів доларів США у 1989 році, у 1991 році вони становили 164,3 мільйони доларів США. Нині збитки оцінюються до мільярда доларів США.

Ситуація на території СНД та країн, які входили до Радянського Союзу, своєрідна, але сьогодні подібна на Західний світ часів становлення і розквіту

хакерського руху там. Хоча комп'ютерна злочинність у СНД почала розвиватися пізніше, однак невизначеність у національному законодавстві та міждержавних документах і усвідомленні боротьби з нею на трансграничному рівні створила сприятливі умови для її розвитку.

Щодо України, умовою формування і розвитку хакерського руху є високий рівень безробіття серед випускників технічних вищих закладів освіти, де викладають поглиблені знання з комп'ютерного програмування.

За останніми узагальненими неофіційними (оперативними) даними хакери в Україні, Росії та інших країнах колишнього Радянського Союзу об'єднані в регіональні групи, мають свої електронні засоби інформації (газети, журнали, електронні дошки об'яв в Інтернеті). Вони проводять електронні конференції, мають свій словник жаргонів, який постійно поповнюється і поширюється за допомогою комп'ютерних бюлетенів, які містять всі необхідні відомості для "підвищення майстерності" початківців - методики проникнення в конкретні системи і способи зламу комп'ютерних програмних систем захисту.

Українські та російські хакери і крекери тісно контактують зі своїми "колегами" з інших країн, співпрацюють з ними, обмінюються досвідом, широко використовуючи для цього канали глобальних телекомунікаційних мереж (Інтернет).

Однією з причин хакерського руху, а також витоку висококваліфікованих кадрів за кордон експерти визначають невідповідність орієнтації при масовій підготовці спеціалістів у вищих навчальних технічних закладах сучасним суспільним ринковим економічним відносинам. При дослідженні української системи підготовки фахівців у сфері комп'ютерної індустрії з'ясовано, що здебільшого у вищих закладах освіти їх готують як виконавців, найманих працівників, а не підприємців. Тобто їх вчать продавати себе у найм, а не на ринкових засадах результати своєї інтелектуальної праці. Вітчизняна вища технічна школа мало приділяє уваги наданню знань підприємницької діяльності та правовій підготовці. Вона готує фахівців-виконавців, які

зорієнтовані на те, що їм держава підприємці (у тому числі іноземні) повинні створити умови для праці.

3.6. Латентність комп`ютерної злочинності

За експертними оцінками, багато комп`ютерних злочинів не виявляють або про них не повідомляють потерпілі (латентні). За оцінками фахівців, в середньому 90% злочинів цього виду поки що залишається поза увагою правоохоронних органів держави.

Достовірні дані збитків від комп'ютерної злочинності визначити важко - ні зловмисники, ні потерпілі не намагаються надавати їм гласності за певних обставин. Одні - через можливу відповідальність за вчинене, а інші - через страх втрати іміджу, ділової репутації тощо. Це також пояснює високий рівень латентності правопорушень і брак про них відомостей у засобах масової інформації. На думку експертів, до широкої громадськості доходить лише 1% від всіх випадків виявлених порушень, що звичайно мають кримінальний характер і приховати які стало неможливо.

Проблема латентності значною мірою пов'язана з об'єктивними і суб'єктивними можливостями правоохоронних органів. Незважена політика держави щодо скорочення штатів правоохоронних органів, переорієнтація їх на нові прояви злочинності, низький рівень матеріального та фінансового забезпечення спричинюють відтік висококваліфікованих кадрів.

Причиною високого рівня латентності комп'ютерної злочинності в Україні також є те, що правоохоронні органи не можуть забезпечити відповідну реакцію на постійно зростаючий обсяг оперативної інформації про комп'ютерні злочини, яку вони мають у повному обсязі опрацювати. Чим більші ресурсні обмеження, тим більший обсяг сигналів про злочини система правоохоронних органів змушена від себе відштовхувати, залишаючи їх у "латентній тіні". Дослідження різних країн на рівні статистичної закономірності свідчать, що зростання злочинності на 2-3% викликає зниження розкриття злочинів приблизно на 1%, що, в свою чергу, збільшує кількість ухилення правопорушників від

відповідальності. На це необхідно зважувати під час оцінки діяльності правоохоронних органів.

Характерною ознакою латентності комп’ютерної злочинності є наступне явище. Нерідко, зафіксувавши спробу проникнення в базу даних державного відомства, при зверненні відповідних правоохоронних органів провайдери, які обслуговують українських абонентів у мережі Інтернет, на прохання знайти і зафіксувати порушника, обмежуються відключенням абонента від мережі. Тим самим приховуються правопорушення від обліку та вжиття заходів щодо притягнення винних до відповідальності. В результаті – створюються умови безкарності та можливості для вчинення повторних правопорушень.

3.7. Збитки від міжнародної комп`ютерної злочинності

Згідно з даними Комісії з попередження злочинності та кримінального права Організації Об'єднаних Націй щорічний економічний збиток від комп'ютерних злочинів, за оцінками експертів, обчислюється мільярдами доларів США.

У сфері електронної торгівлі із застосуванням пластикових карток, за даними міжнародних фінансових організацій, з 1998-1999 років спостерігається зростання правопорушень приблизно на 54%. Тільки втрати VISA по Україні оцінюються у сумі 1459,842 мільйонів доларів США за 1999-2000 роки.

Дослідження свідчать, що тільки обсяг операцій у разі електронного передавання валюти вказує на те, що потенційні втрати значно вищі, ніж при тих же самих операціях з використанням паперових документів. Втрати ж окремо взятої держави в таких випадках за лічені хвилини можуть досягати дуже значних розмірів, якщо держави не будуть вживати упереджувальних заходів.

Збитки виробників комп’ютерних програмних продуктів внаслідок порушення авторського права та інших прав інтелектуальної власності щодо

комп’ютерного програмного забезпечення щорічно становлять близько 11 млрд доларів США.

Загальні об’єктивні збитки в Україні обрахувати неможливо через брак офіційних методик їх обчислення та таких показників державної статистики. Проте є підстави вважати, що невизначеність стосовно протидії економічній кіберзлочинності - одна із головних причин повільного економічного зростання національного багатства України.

Розділ. 4. Прогноз розвитку комп’ютерної злочинності

Розвиток міжнародних (регіональних, континентальних, глобальних) комп`ютерних мереж на базі телефонного, радіо- та супутникового зв’язку створює не тільки можливість розвитку міжнародного інформаційного співробітництва, а й має тенденцію до розширення можливості вчинення правопорушень.

Інформація, сконцентрована в комп’ютерних системах, об`єктивно полегшує роботу, збільшує швидкість її розповсюдження та отримання через трансграничні, всесвітні комп’ютерні мережі на зразок Інтернет.

Прогрес у сучасних (нових, новітніх, високих) технологіях здобування та обробки інформації надає найкращі, найзручніші позиції її власником щодо економічного, політичного, культурологічного, ідеологічного чи військового наступу.

Комп’ютерна злочинність, у тому числі така, що має ознаки організованої, є однією з характерних і закономірних ознак, негативним відображенням інформаційного суспільства, інформаційної цивілізації і щодо сфери суспільних відносин має і матиме наступні форми:

Використання комп’ютерних інформаційних технологій для вчинення традиційних злочинів. Зокрема, спостерігається тенденція до використання комп’ютерних інформаційних технологій для вчинення таких традиційних злочинів: вимагательство, порушення волі, честі та гідності особи, шпигунство, пропаганда війни, диверсії, організації масових

безпорядків тощо. Особливо активно комп'ютерні інформаційні технології використовуються, поряд з іншими засобами злочинного посягання, для планування традиційних злочинів та "відмивання" коштів, отриманих злочинним шляхом.

Об`єктивна недосконаліть технічного захисту комп`ютерних мереж стає причиною розкрадання коштів у великих обсягах шляхом їх електронного переказу за вигадані послуги, на фіктивні рахунки, у тому числі через електронну міжнародну банківську систему платежів усього світу. Особливо це характерно для переказів коштів на поточні рахунки до тих країн, де уряди не особливо турбують себе запитами та іншими формами перевірки їх походження (міжнародні офшорні зони, міжнародні "вільні економічні зони", країни "відмивання тіньових прибутків" тощо).

Комп'ютерна злочинність у сфері економіки:

Шахрайство в Інтернет-торгівлі організованих злочинних формувань. Використовуючи отримані злочинним шляхом номера кредитних карток громадян різних країн злочинні групи здійснюють замовлення товарів в інших державах через так звані електронні магазини (крамниці).

Крадіжки із застосуванням комп`ютерних технологій організованими злочинними угрупованнями. Збитки від крадіжок, які були вчинені за допомогою транснаціональної мережі Інтернет, щорічно оцінюються до десятка мільярдів доларів. По мірі розширення інформатизації України та розвитку інформаційних суспільств у різних країнах можна прогнозувати зростання таких кіберзлочинів.

Трансграничне "нелегальне інформаційне брокерство" – розглядається у міжнародних відносинах як різновид організованої комп'ютерної злочинності, що має тенденцію до зростання. Особи, які цим займаються за допомогою хакінгу (злому комп'ютерних систем із застосуванням спеціально створених комп'ютерних програм), долають системи технічного захисту інформації в автоматизованих (комп`ютерних)

системах - комп`ютерних мережах, отримують з автоматизованих баз даних інформацію, а потім її продають.

Покупцями виступають як конкуруючі організації (фірми), так і організації потерпілі (форма шантажування, вимагательства тощо).

Організоване промислове (комерційне, підприємницьке) шпигунство. На думку фахівців, збитки від розвідувальної діяльності конкурентів, які використовують методи шпигунства організованих злочинних формувань, становлять у світі до 30% всіх збитків, а це - мільярди доларів США.

Масштаби організованого злочинної діяльності можна оцінити хоча б за такими фактами: на одній з багатьох виставок - продажу апаратури технічної розвідки та контррозвідки було продано 70 тисяч одиниць апаратури добування інформації і тільки одиниці їх пошуку і боротьби з ними. А всього на виставці було виставлено більш ніж 2000 видів різних приладів технічного добування і захисту інформації, яка, як правило коштує дуже дорого.

Крадіжки грошей та матеріальних цінностей через інформацію, яка циркулює в електронній (комп'ютерній) формі. Цей вид антисоціальних проявів проти відносин права власності стає таким же небезпечним, як викрадення дітей, вимагання, тероризм, торгівля наркотиками тощо.

Економічне шпигунство конкурентів за допомогою комп'ютерних інформаційних технологій. Як засіб інформаційної боротьби застосовується з метою завоювання кращих позицій на ринку, в суспільних економічних відносинах. Як вид злочинності - зумовлений постійним нарощуванням інформатизації установ підприємств, організацій всіх форм власності. Інформація, яка була здобута внаслідок економічного шпигунства у кіберпросторі, допомагає знайти шляхи до отримання прибутків швидше і дешевше. Все це не виключає можливості щодо зростання злочинних проявів.

Шахрайство у сфері електронної комерції (е-комерції) через Інтернет. Існують різні класифікації видів шахрайства з використанням комп'ютерних технологій. Найбільш прийнятна з них така:

1) шахрайство з втраченими і викраденими пластиковими електронними картками – 72,2%;

2) шахрайство з підробленими картками – 20,5%;

3) шахрайство з картками, не отриманими законним держателем – 2,8%;

4) шахрайство з використанням рахунка – 1,4%;

5) інші форми шахрайств – 3,1%.

Аналіз співвідношення видів шахрайств в е-комерції за сервісними підприємствами (підприємствами, що надають послуги) свідчить, що найчастіше відбуваються антисоціальні прояви через:

ресторани – 26,4%;

готелі (мотелі) – 25%;

магазини – 20,7%;

бари – 10,6;

телефонні послуги – 7,4%.

До їх числа також входять підприємства комерційної мережі, які обслуговують населення, установи, організації, підприємства з застосуванням так званих електронних пластикових карток платежів.

**Комп`ютерне хуліганство.** Серед антисуспільних проявів у кіберпросторі, зокрема в Інтернет, набули поширення комп`ютерні хуліганства, які в подальшому збільшуватимуться. Цей вид антисоціальної діяльності не знайшов адекватного відображення як правопорушення в юридичній діяльності щодо захисту на рівні законодавства багатьох країн. Способи його вчинення різноманітні: від розповсюдження шкідливих комп’ютерних програм (комп`ютерних вірусів) з хуліганських мотивів, до поширення образ, наклепів щодо окремих осіб, організацій, держав у мережі Інтернет. В деяких країнах розглядається як аналог телефонного та радіохуліганства.

Хакерський рух. У багатьох розвинутих у інформаційному відношенні країнах спостерігається зростання такого соціального явища, як хакерський рух. Як зазначалося вище, а також при дисбаланси попиту і пропозиції на ринку праці високо кваліфікованих спеціалістів у сфері комп'ютерного програмного забезпечення, та низького рівня оплати праці зазначених фахівців в Україні можливе зростання цього негативного явища для суспільства.

Кібервійни, кіберборотьба, боротьба у кіберпросторі (інформаційні війни, інформаційна боротьба). Вони у оборонних, військових доктринах багатьох країн розглядаються як перспективний засіб боротьби антагоністичних соціальних систем: окремих суспільних угруповань, держав, їх військових блоків, союзів тощо. За певних обтяжуючих обставин, на міжнародному рівні, ведення інформаційної війни може розглядатися як злочини проти людства, безпеки існування світової чи локальної (регіональної) цивілізації.

Комп`ютеризація арсеналів ядерної зброї, ракет стратегічного призначення, що здатні нести бойові заряди масового знищення об`єктивно створює умови для переростання інформаційної боротьби до ядерної через внесення збоїв в інформаційні системи, які забезпечують застосування ядерної зброї.

Кіберборотьба є одним із засобів ведення інформаційної війни з метою ідеологічного та психологічного впливу на свідомість окремих індивідів, соціальних спільнот, народу, держави, розпалення національної, етнічної чи релігійної ворожнечі, підриву територіальної цілісності держави, міждержавних політичних та економічних союзів тощо. У зазначеному контексті кіберборотьба є різновидом загрози національній безпеці та безпеці мирного міжнародного співіснування.

Застосування Інтернет терористичними організаціями. У багатьох країнах спостерігається зростання рівня використання Інтернет терористами, у тому числі релігійними фундаменталістами та сектами. Карти, плани, фотографії мішеней і відповідні інструкції приховано і відкрито розміщуються в чатах (комп'ютерних сторінках в Інтернет), порнографічних бюлетенях та інших популярних сайтах глобальної мережі. В окремих випадках, при потребі файли зашифровуються так, що тільки самі терористи можуть отримувати інформацію з них.

Правоохоронними органами багатьох країн постійно фіксується інформація, яка свідчить про використання терористичними групами Інтернет у плануванні своїх злочинних операцій.

Комп'ютерний тероризм організованих злочинних формувань. У широкому розумінні - діяльність окремих екстремістських організацій націоналістичного, сепаратиського, колобораціоніського, релігійного, політичного змісту тощо. У вузькому – вчинення нападів за допомогою комп'ютерних технологій на автоматизовані (комп'ютерні) системи органів державної влади, громадських організацій, різних установ, підприємств або фізичне руйнування чи пошкодження таких систем з метою вчинення диверсій (ослаблення держави).

Вчинення кібертерористичних актів - застосування комп'ютерної техніки для порушення роботи автоматизованих (комп'ютерних) систем, що спричинює дії, які створюють небезпеку для життя чи здоров'я людини або спричинюють значну майнову шкоду чи призводять до інших тяжких наслідків з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших

поглядів терориста, а також погроза вчинення зазначених дій з тією самою метою.

Спектр застосування комп'ютерних засобів для вчинення терористичних актів різноманітний, особливо він стає небезпечним по мірі розвитку міжнародної системи Інтернет, інтеграції її з супутниковим та радіозв'язком, стільниковою телефонією, супутниковим телебаченням, зростання інформатизації різних сфер державного управління, закладів охорони здоров'я, освіти, культури тощо.

Розділ 5. Міжнародна боротьба з кіберзлочинністю

5.1. Організаційні заходи міжнародного співтовариства щодо боротьби з комп'ютерною злочинністю у світі

Генеральний Секретаріат Інтерполу у 1994 році рекомендував всім країнам - членам організації створити національні центральні консультативні пункти з проблем комп'ютерної злочинності (National central reference point) та закріпити конкретних працівників для роботи з інформацією про комп'ютерні злочини для оперативного обміну такою інформацією між країнами.

Ці пункти створено, як правило, в апаратах Національних Бюро Інтерполу, або у спеціалізованих підрозділах, які ведуть боротьбу з комп'ютерною злочинністю, або у підрозділах боротьби зі злочинами у сфері економіки.

5.2. Участь України у міжнародній організації боротьби з комп'ютерною злочинністю

На базі НЦБ Інтерполу в Україні 17 вересня 1996 року був створений національний консультативний пункт щодо боротьби з кіберзлочинністю . Це дало можливість:

накопичити матеріал про законодавче регулювання боротьби з комп'ютерною злочинністю у різних країнах;

узагальнити досвід організації попередження, розкриття і розслідування комп'ютерних злочинів;

підготувати низку аналітичних оглядів і публікацій з цих питань;

ознайомити працівників МВС, прокуратури, суду з цим новим для України видом злочинів;

внести конкретні пропозиції щодо удосконалення кримінального законодавства України.

Розділ 6. Проблеми правового регулювання суспільних інформаційних відносин в умовах інформатизації України та шляхи їх подолання

6.1. Проблеми правового регулювання суспільних інформаційних відносин в умовах інформатизації України

У сфері суспільних інформаційних відносин нормотворення в Україні здійснюється через вирішення окремих проблем в окремих законах та підзаконних нормативних актах фрагментарно. В той же час значний масив норм щодо інформації розміщено в кодифікованому законодавстві, зокрема в цивільному, адміністративному, трудовому, кримінальному. Таким чином, в Україні сформувалася національна специфічна змішана доктрина права, яка поєднує в собі елементи англо-американської та європейської континентальної юридичних систем.

За наявною доктриною, серед недоліків законотворчої діяльності в Україні визначаються такі:

1. Правотворчий процес на всіх рівнях органів державної влади нерідко здійснюється без узгодження з чинним законодавством, не враховується специфіка національної ментальності, правової культури систематизації права, які є основою правосвідомості населення, інші особливості соціального та державного життя.

2. Різні закони та підзаконні акти, що регулюють суспільні відносини, об'єктом яких є інформація, приймались у різні часи без узгодження

понятійного апарату, тому вони мають низку термінів, які не є достатньо коректними, а отже, розуміються неоднозначно учасниками суспільних інформаційних відносин. Деякі категорії взагалі не мають чіткого визначення свого змісту, що призводить до їх неоднозначного застосування на практиці. Наприклад, "інформація", “таємна інформація” і “таємниця”, "документ" і “документована інформація”, "майно" і "власність", “інтелектуальна власність”, "володіння", "автоматизована система" тощо. Це, в свою чергу, породжує соціальні конфлікти (правопорушення) в інформаційних відносинах між їх учасниками та створює умови для уникнення від відповідальності правопорушників, що негативно впливає на формування високої культури правовідносин на рівні найкращих здобутків світової інформаційної цивілізації.

3. Значна кількість юридичних норм, які регулюють суспільні інформаційні відносини, розпорошена по різних законах та підзаконних нормативних актах, що ускладнює їх пошук, аналіз та узгодження для практичного застосування.

4. Має місце розбіжність щодо розуміння структури системи законодавства в сфері інформаційних відносин та підходів до її формування. Нерідко через окремі закони в систему законодавства вносять норми підзаконних нормативних актів, що суперечить положенням Конституції України. Це викликає в практиці правозастосування колізію норм - ігнорування норм закону на користь норм підзаконного акта.

5. Нові юридичні норми в сфері суспільних інформаційних відносин нерідко не узгоджені з раніше прийнятими, що призводить до правового хаосу, падіння авторитету публічного права, правового нігілізму суб’єктів суспільних інформаційних відносин.

Сукупність правових норм у сфері суспільних інформаційних відносин, визначених у законах і підзаконних актах, досягли за кількістю критичного стану (критичної маси), що зумовлює необхідність легального виділення їх в окрему галузь законодавства – інформаційне законодавство.

6.2. Удосконалення нормативно-правового забезпечення і регулювання боротьби з комп'ютерною злочинністю

Одним із способів подолання проблем правового регулювання і забезпечення суспільних інформаційних відносин є законодавча систематизація норм інформаційного права та адаптація його до нових сфер суспільних правовідносин, об'єкт яких становить інформація в умовах інформатизації України.

Шляхи подолання проблем правового забезпечення і регулювання боротьби з комп'ютерною злочинністю в Україні, як складової суспільних інформаційних відносин:

подальше формування інформаційного законодавства в Україні як міжгалузевої комплексної інституції на основі інститутів конституційного, адміністративного, цивільного, трудового та кримінального законодавства;

адаптація і введення в правову систему України позитивних здобутків міжнародного досвіду правового регулювання боротьби з комп'ютерною злочинністю способом рецепції, імплементації та ратифікації юридичних норм на принципі державного суверенітету, його складової інформаційного суверенітету, у системі національного інформаційного законодавства.

Частина 2. Стратегічні засади боротьби з комп'ютерною злочинністю в Україні

Розділ 7. Державна політика України щодо боротьби з комп'ютерною злочинністю

7.1. Організаційно-правові засади державної політики України щодо боротьби з комп'ютерною злочинністю

Правову основу державної політики України щодо боротьби з комп'ютерною злочинністю становить Конституція України, у тому числі положення, визначені статтею 17 Конституції України: захист суверенітету і територіальної цілісності України, забезпечення її економічної та

інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу.

Розвиток положень Конституції України знаходить відображення у законодавстві України.

Державна політика щодо боротьби з комп'ютерною злочинністю визначається також з урахуванням норм міжнародного права, у тому числі міжнародного інформаційного права, що знайшло відображення у міждержавних угодах, у тому числі:

Статуту ООН;

Статуту ООН з питань освіти, культури і науки;

Статуту Ради Європи;

Статуту Світової організації інтелектуальної власності;

Окремих міждержавних угод Співдружності незалежних держав.

Протидія комп'ютерній злочинності та комп'ютерним злочинам здійснюється на засадах міжнародного права щодо інтелектуальної власності.

У цій сфері суспільних відносин державна політика України спрямована згідно з положеннями таких міждержавних актів:

Угода про співробітництво в галузі охорони авторського права і суміжних прав;

Угода про співробітництво з припинення правопорушень у сфері інтелектуальної власності;

Бернська конвенція про охорону літературних і художніх творів (Паризький акт від 24 липня 1971 року, зі змінами від 2 жовтня 1979 року);

Договір про закони щодо товарних знаків;

Мадридська Конвенція з міжнародної реєстрації фабричних та товарних знаків 1891р.;

Женевська Всесвітня конвенція з авторського права 1952 р.;

Римська Конвенція охорони виробників фонограм та транслюючих (повідомляючих) організацій 1961р. ;

Вашингтонський Договір з патентної кооперації (PCT) 1970 р.;

інші багатосторонні міждержавні угоди.

У сфері інших міжнародних інформаційних правовідносин державна політика України грунтується на таких міжнародних актах:

Статут і Конвенція Міжнародного союзу електрозв'язку;

Статут Всесвітнього поштового союзу (а також Протоколи до нього);

Угода щодо співробітництва у розвитку та використанні систем стільникового рухомого зв'язку;

Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля;

Конвенція про правонаступництво держав у відношенні державної власності, державних архівів та державних боргів (Відень, від 08.04.83);

Конвенція з розповсюдження сигналів, що несуть програму, що передаються через супутники (Брюссель, 1974 р.);

Європейська хартія регіональних мов або мов меншин;

Правила визначення країни походження товарів (Додаток №1, затверджені Рішенням Ради глав Урядів СНД від 42.09.1993 р.);

Міжнародні нормативні акти у сфері економічних відносин, міжнародної банківської, комерційної, підприємницької діяльності;

інші міждержавні угоди, введені у правову систему України відповідно до принципів та звичаїв міжнародного права.

7.2. Профілактика комп’ютерної злочинності

Профілактика комп’ютерної злочинності в Україні здійснюється відповідно до чинного адміністративного, цивільного, трудового та кримінального законодавства.

За структурою профілактика комп’ютерної злочинності поділяється на загальну, групову та індивідуальну.

Мета профілактики комп'ютерної злочинності полягає у виявлення організаційних, технічних і правових недоліків щодо охорони та захисту комп'ютерної інформації та систем, де вона циркулює.

Важливими аспектами профілактики кіберзлочинів є виявлення соціальних, соціально-економічних, освітніх та інших причин та умов вчинення таких злочинів та їх усунення.

Основні заходи загальної профілактики кіберзлочинів визначаються державною політикою щодо захисту інформації, інформаційної безпеки людини, суспільства, держави.

З метою організації координації протидії комп'ютерній злочинності Президентом України, Кабінетом Міністрів України, відповідно до визначеної у законодавстві їх компетенції, утворюються міжвідомчі структури (комітети, робочі групи щодо розробки проектів нормативно-правових та інших актів державної влади).

Провідний відповідальний орган республіканської виконавчої влади в Україні, який визначає, координує і реалізує державну політику у сфері інформаційної безпеки, є Служба безпеки України.

Провідний відповідальний орган щодо попередження проявів використання комп'ютерної мережі електронних платежів та розрахунків у сфері економічних відносин та банківської діяльності є Міністерство фінансів України та Національний банк України.

Окремі аспекти щодо реалізації державної політики у сфері інформаційної безпеки знаходять вираз у адміністративних нормативних актах органів центральної виконавчої влади.

Нормативні акти міністерств і відомств щодо профілактики кіберзлочинів адміністративними засобами та заходами грунтуються на таких нормативно-правових актах органів виконавчої влади, у тому числі:

Накази Державної служби України з питань технічного захисту інформації:

"Про затвердження Інструкції щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за їх дотриманням" N46 від 23.05.1994 р.;

Інструкція про порядок надання дозволу на використання імпортних засобів ТЗІ, а також продукції, яка містить їх у своєму складі, затверджена наказом № 13 від 31.05.1995 р.;

"Про нормативні документи" N25 від 09.06.1995 р.;

"Про затвердження нормативного документу" N35 від 10.07.1995 р.;

ТПКО-95 (Тимчасове положення про категоріювання об'єктів). Додаток таємно.;

ТР ТЗІ - ПЕМВН-95 (Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань та наводок);

ТР ЕОТ-95 (Тимчасові рекомендації з технічного захисту інформації в засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок);

Про затвердження Положення про порядок опрацювання, прийняття та скасування міжвідомчих нормативних документів системи технічного захисту інформації N44 від 01.07.1996 р.;

Тимчасові рекомендації щодо розроблення розділу із захисту інформації в технічному завданні на створення автоматизованих систем. (ТРАС-96) № 47 від 03.07.1996 р.;

Правила побудови, викладення, оформлення та позначення нормативних документів системи ТЗІ. НД. ТЗІ 1.6-001-96. (Наказ № 51 від 26.07.1996 р.;

Наказ *Державного митного комітету України* Положення про електронну інформацію в митній системі України від 08.02.1996 р.;

Нормативні акти *Держстандарту України*, у тому числі:

ДСТУ 1.3-93. Порядок розроблення, побудови, викладу, оформлення, узгодження, затвердження, позначення та реєстрації технічних умов (затверджено та введено в дію наказом Держстандарту № 116 від 29.07. 1993р.);

КНД 50-009-93. Типова побудова технічних умов. Методичні вказівки (затверджено та введено в дію Наказом Держстандарту № 116 від 29.07. 1993р.);

ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення (введено в дію Наказом Держстандарту № 423 від 11.10. 1996р.);

ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт (введено в дію Наказом Держстандарту № 511 від 19.12. 1996р.);

Нормативні акти *органів місцевого самоврядування та місцевих державних адміністрацій* щодо профілактики кіберзлочинів та інших правопорушень з використанням комп'ютерної техніки та комп'ютерних продуктів видаються на підставі законодавства України, нормативно-правових актів Президента України та нормативно-правових актів органів центральної виконавчої влади.

Нормативні *акти установ, підприємств, організацій* усіх форм власності щодо профілактики кіберзлочинів визначаються їх установчими (статутними) документами (статутами, уставами, положеннями тощо) відповідно до законодавства та підзаконних нормативно-правових актів органів державної влади.

7.3. Основні організаційні напрями удосконалення протидії комп'ютерній злочинності в Україні з урахуванням міжнародного досвіду

Державні правоохоронні установи у різних країнах світу утворюють спеціалізовані підрозділи, кількість яких постійно зростає, для збирання та

аналізу так званих “електронних” чи “комп’ютерних” доказів. Цю функцію також виконують численні спеціальні лабораторії судової експертизи.

Зазначені обставини є одним із обгрунтувань формування спеціальних підрозділів по боротьбі зі злочинами, що вчиняються з використанням комп’ютерних технологій.

Досвід багатьох країн свідчить, що комп’ютерні злочини мають розслідуватись лише тими підрозділами чи співробітниками правоохоронних органів, які мають спеціальні навички для ведення таких справ та пройшли відповідну підготовку. Це пов’язано з тим, що робота з комп’ютерним обладнанням вимагає спеціальних знань. Серйозні проблеми, які призводять до значних витрат, можуть виникнути, якщо справу з цією технікою матиме некваліфікована особа.

Існує нагальна потреба у розгортанні спеціалізованих підрозділів в системі правоохоронних органів України та у підготовці кваліфікованих працівників не тільки в юридичних, а й в економічних і технічних аспектах.

Структурним підрозділам органів державної виконавчої влади слід розробити організаційно-правові заходи щодо взаємодії і підтримки діяльності українських громадських формувань, асоціацій, союзів недержавних підприємств, установ, організацій щодо протидії комп’ютерної злочинності:

Академією правових наук України (Науково-дослідним центром правової інформатики, Харківським центром вивчення організованої злочинності та іншими);

Асоціацією кримінологів України;

Українською Міжбанківською Асоціацією Членів Юропей Інтернешнл;

іншими неурядовими організаціями.

Розділ 8. Організаційно-управлінське забезпечення боротьби з комп’ютерною злочинністю в Україні

Організаційно-управлінське забезпечення боротьби з комп'ютерною злочинністю в Україні має здійснюватися через:

формування функціональних організаційних структур у статусі управлінь по боротьбі зі злочинами у сфері використання комп'ютерних інформаційних технологій в центральних апаратах Міністерства внутрішніх справ, Служби безпеки, Державної податкової адміністрації (податковій міліції) України;

створення навчальних структур (центрів, спеціалізованих груп тощо) для спеціальної підготовки співробітників функціональних служб щодо боротьби з комп'ютерною злочинністю (оперуповноважених, слідчих та криміналістів);

поетапне розширення функціональних структур боротьби з комп'ютерною злочинністю, тобто створення:

міжрегіональних підрозділів;

спеціалізованих підрозділів на рівні обласних управлінь;

структурних одиниць в системі міськрайорганів.

Розділ 9. Матеріально-фінансове забезпечення боротьби з комп'ютерною злочинністю

Матеріально-фінансове забезпечення боротьби з комп'ютерною злочинністю визначається з урахуванням економічного стану України, відповідно до програм боротьби зі злочинністю, окремих її видів з державного та місцевих бюджетів.

На умовах співвідношення потреб та інтересів додаткове матеріально-технічне забезпечення та фінансування може здійснюватися недержавними, приватними установами, підприємствами та організаціями, фондами громадськими об'єднаннями, у тому числі зі спонсорської та іншої допомоги, а також приватними (фізичними) особами у порядку, визначеному законодавством України.

Розділ 10. Наукове забезпечення боротьби з комп'ютерною злочинністю в Україні

10.1. Основні засади наукового забезпечення боротьби з кіберзлочинністю

В умовах розвитку інформаційного суспільства, інформатизації в Україні суспільні інформаційні відносини, система правових норм, їх регулювання потребують постійного моніторингу (відслідковування) щодо їх адекватності до нових умов і узгодження з іншими новими соціальними відносинами, зокрема щодо виявлення проблем у цих відносинах з науковим обгрунтуванням їх вирішення. Це, в першу чергу, потрібно для упередження негативних соціальних наслідків інформатизації, у тому числі щодо комп'ютерної злочинності.

10.2. Наукові положення щодо систематизації інформаційного законодавства України

В основу законодавчої інкорпорації покладаються відпрацьовані юридичною наукою і перевірені практикою норми законодавства України.

При систематизації інформаційного законодавства увага повинна звертатися на визначення структури, місця юридичних норм в системі правового регулювання. Необхідно чітко визначити суб'єкти і об'єкти інформаційних відносин, правила поведінки учасників, їх права та обов'язки.

На рівні наукової доктрини:

1. Суспільні інформаційні відносини складають умовно автономну галузь (сферу) суспільних відносин, які тісно переплітаються з іншими сферами суспільних відносин.

2.Інформаційне законодавство є галуззю законодавства, яке тісно пов`язане з іншими галузями законодавства України.

3. Інформаційне законодавство регулює суспільні правовідносини щодо інформації як форми виразу інших правовідносин: у засобах масової інформації, освіті, культурі, бібліотечній та архівній справі, науковій та науково-технічній діяльності, праві інтелектуальної власності, інформатизації, інформаційно-аналітичному забезпеченні діяльності органів влади всіх рівнів

соціального управління (представницької, виконавчої та судової), захисту інформації, державної таємниці, інформаційної безпеки тощо.

10.3. Розвиток теоретико-правової бази та практики правового регулювання суспільних інформаційних відносин

Розвиток теоретико-правової бази та практики правового регулювання суспільних інформаційних відносин в нашій країні потрібно здійснювати з урахуванням зарубіжного досвіду та міжнародного права. Особлива увага повинна звертатися на виявлення та дослідження недоліків, щоб уникнути їх у правотворчій та правозастосовчій діяльності, запобігати негативним для суспільства наслідкам інформатизації.

10.4. Постійний моніторинг небезпечних соціогенних загроз безпеці суспільним інформаційним відносинам

Постійний моніторинг передбачає відслідковування та визначення найнебезпечних соціогенних, зокрема криміногенних, загроз безпеці суспільним інформаційним відносинам, відповідне реагування на ці загрози, регулювання захисту інформації, у тому числі в автоматизованих (комп'ютерних) системах.

Моніторинг здійснюється на рівні відповідних уповноважених структур органів державної виконавчої влади, наукових установ. Для забезпечення об'єктивності інформації державою заохочується ініціатива громадськості щодо формування громадських і приватних науково-практичних структур дослідження комп'ютерної злочинності.

10.5. Принципи наукового забезпечення правотворчої діяльності

Провідними принципами наукового забезпечення правотворчої діяльності щодо систематизації в сфері соціальних інформаційних відносин є:

системний та комплексний підходи у вирішенні проблем правотворчості;

фундаментальне та прикладне теоретичне обгрунтування новацій (понять, категорій тощо);

демократизм - залучення широкого кола вітчизняних фахівців до обговорення проблем інформаційного законодавства та суспільних інформаційних відносин;

недопустимість необгрунтованого копіювання зарубіжного досвіду;

повага та гуманне ставлення до людини, її честі, гідності, репутації;

презумпція невинності людини, громадянина, приватної особи.

Формування правової доктрини гармонізації національного інформаційного права України з міжнародним інформаційним правом.

Фахівці, які залучаються до систематизації інформаційного законодавства, повинні володіти знаннями в галузі права та інформатики, теорії і практики організації та управління соціальними системами в умовах інформатизації.

Доктринально визнається багатооб'єктність юридичних норм, законодавства в юридичній кваліфікації суспільних інформаційних відносин.

Напрями, підцілі, завдання систематизації інформаційного законодавства повинні чітко формуватися відповідно до теорії системи підцілей ("дерева цілей").

10.6. Методологічні підходи систематизації інформаційного законодавства України

1. Правотворення повинно ґрунтуватися на основі методології системного і комплексного підходів - теорії формування комплексних ієрархічних гіперсистем інформаційного законодавства: розвиток конституційних норм має знаходити вираз у системоутворювальних законодавчих актах, які регулюють суспільні інформаційні відносини в Україні. Системоутворювальним законодавчим актом у майбутньому повинен стати прийнятий Верховною Радою України Кодекс про інформацію, в якому будуть розвиватися визначені в Конституції України положення про суспільні інформаційні правовідносини.

Систематизація інформаційного законодавства має вирішити такі завдання-цілі:

розвивати норми і принципи правового регулювання суспільних відносин, що визначені в Конституції України;

враховувати ратифіковані Україною нормативні акти міжнародного права (міждержавні угоди, конвенції);

легалізувати позитивні звичаї в сфері інформаційних відносин та норми суспільної моралі, загальнолюдські цінності, визначені Організацією Об'єднаних Націй в Декларації прав людини та інших загальноприйнятих міждержавних нормативних актах.

2. Методологічною базою правотворення інформаційного законодавства України є юридична доктрина щодо умовного поділу права на галузі за такою принциповою моделлю: основа - конституційне право; його положення знаходять паралельний розвиток (відповідно до методів правового регулювання і захисту прав) в адміністративному, цивільному, трудовому та кримінальному праві, інших підсистемах національного права України, в нормах яких інформація виступає як опосередкований, додатковий (факультативний) предмет регулювання суспільних відносин.

3. Домінуючою в методології систематизації суспільних інформаційних відносин в Україні є доктрина сучасного вітчизняного конституційного права (основа - Конституція України) та прогресивних здобутків міжнародного права щодо верховенства права людини.

4. Систематизація інформаційного законодавства має проводитися методом агрегації: удосконалення окремих правових норм чи створення нових міжгалузевих правових інститутів через непорушення цілісності та призначення інформаційного законодавства, удосконалення його дієвості в цілому, створення нової системної якісті, яка не характерна окремим його складовим.

Провідними функціями систематизації інформаційного законодавства України є:

регулятивна - визначення зобов'язань, прав та обов'язків суб'єктів, регулювання суспільних інформаційних відносин;

нормативна - визначення норм, правил поведінки суб'єктів інформаційних відносин;

охоронна - визначення гарантій та меж правомірної поведінки, форм та умов, за якими діяння утворюють правопорушення (делікти), відповідальності за них відповідно до норм цивільного, адміністративного, трудового, кримінального законодавства;

інтегративна - системне поєднання комплексу визначених юридичних норм, які регулюють інформаційні відносини в Україні; поєднувальна ланка між провідними традиційними галузями права (конституційним, цивільним, адміністративним, трудовим та кримінальним) щодо застосування їх методів та принципів правового регулювання та захисту в сфері інформаційних відносин;

комунікативна - зазначення в окремих статтях посилань на наявні законодавчі акти, створення підсистем різних міжгалузевих підінститутів (субінститутів) права, в яких інформація виступає як форма виразу правовідносин (банківське, комерційне, господарське, авторське право, право інтелектуальної власності тощо).

Провідні завдання систематизації інформаційного законодавства:

визначення консенсусу (згоди) в суспільних стосунках, узгодженості розуміння та застосування юридичних норм, правомірної поведінки учасників інформаційних відносин;

забезпечення інформаційного суверенітету, незалежності України у міжнародних стосунках;

забезпечення інформаційної безпеки громадян, їх об'єднань, суспільства та держави як складових національної безпеки України;

визначення правомірної поведінки учасників інформаційних відносин в Україні;

захист інформації від несанкціонованого доступу, витоку, блокування, знищення, підробки, модифікації, перекручення незалежно від технологій обробки та сфер суспільних відносин (особливо в системі інформаційно-аналітичного забезпечення органів державної влади, у банківській, комерційній та інших сферах господарської діяльності).

10.7. Вихідні положення структури інформаційного законодавства України та правового регулювання протидії комп'ютерній злочинності

Основні засади протидії кіберзлочинності поряд з кримінальним законодавством мають знайти закріплення в інших законодавчих актах, у тому числі щодо визначення основних понять та категорій, які вживаються у кримінальному законодавстві.

Відповідно до традицій систематизації законодавства України система інформаційного законодавства України повинна знайти відображення на рівні Кодексу України про інформацію, який структурно має складатися з двох частин (які при необхідності, можуть поділятися на книги):

Частина І. Загальна частина (Загальні положення);

Частина ІІ. Особлива частина (Особливості регулювання інформаційних відносин щодо галузей (сфер) суспільної діяльності).

Кожна з частин поділяється на розділи, розділи, за необхідності, на глави, які складаються з окремих статей.

Структура статті складається з чіткого формулювання диспозиції суспільних правовідносин між їх суб'єктами. В статтях, в яких визначаються правопорушення, повинно бути обов'язкове посилання на вид відповідальності: відповідно до Цивільного кодексу, Кодексу Законів про працю, Кодексу про адміністративні правопорушення, Кримінального кодексу.

Модельні зразки:

"...покарання за це правопорушення настає у відповідності зі статтею… Кодексу про адміністративні правопорушення України",

"...відповідальність настає у порядку, визначеному статтями… Кримінального кодексу України",

"...матеріальна відповідальність настає у порядку, визначеному Цивільним кодексом України",

"...відповідальність настає відповідно до Кодексу законів про працю".

У Цивільному кодексі, Кодексі Законів про працю, Кодексі про адміністративні правопорушення створюються відповідні розділи чи глави щодо питань регулювання та відповідальності за правопорушення суспільних інформаційних відносин з посиланням на норми інформаційного законодавства України.

Розділ 11. Напрями правового регулювання соціальних інформаційних відносин

Основні напрями правового регулювання соціальних інформаційних відносин такі:

1. Визначення та правове закріплення нових напрямів державної політики в галузі соціальних інформаційних відносин в умовах інформатизації, у тому числі щодо боротьби з комп’ютерною злочинністю.

2. Забезпечення реалізації прав осіб (фізичних та їх об’єднань) на режим доступу до інформації, зокрема особистих (персональних) даних - інформації про громадян та організації за умов інформатизації державних органів управління та суспільства в цілому.

3.Забезпечення умов для розвитку і захисту всіх форм власності на інформацію та інформаційні ресурси, права інтелектуальної власності, у тому числі від комп’ютерних злочинів.

4. Забезпечення співвідношення інтересів суб'єктів суспільних інформаційних відносин у сфері національної безпеки, її складових, інформаційної та економічної безпеки.

5. З метою боротьби з поширенням наклепів і образ, захисту честі, гідності та ділової репутації тощо підлягає визнанню засобом масової інформації окремих регіональних, національних та глобальних комп'ютерних мереж, в тому числі таких як Інтернет (електронних газет та журналів, рекламних та інформаційних сторінок установ, організацій підприємств тощо), подібно до радіо і телебачення.

6. Визначення на рівні законодавства інформаційних правовідносин, що виникають при використанні комп'ютерних мереж загального користування, як складової державного юридичного захисту прав і свобод людини.

7. Імплементація норм міжнародного права здійснюється з урахуванням вітчизняної доктрини права щодо поділу його на провідні галузі права: публічне і приватне; а також конституційне, адміністративне, цивільне, трудове і кримінальне право та міжгалузеві комплексні інститути права.

Метою систематизації інформаційного законодавства України є створення чіткої структури правового регулювання суспільних відносин між їх суб'єктами щодо інформації, забезпечення співвідношення потреб та інтересів людини, соціальних спільнот та держави.

Щодо боротьби з кіберзлочинністю зазначені заходи, на умовах комплексного підходу, будуть мати характер профілактики комп'ютерних злочинів.

Розділ 12. Основні організаційні засади щодо систематизації інформаційного законодавства України

1. Відповідно до законодавства України здійснення заходів щодо систематизації інформаційного законодавства покладається на визначені Верховною Радою України її Комітети.

2. За участю Президента України, Кабінету Міністрів України, Національної академії наук України, Академії правових наук України, провідних наукових закладів України формуються робочі група вітчизняних фахівців у галузі інформатики, інших суспільних інформаційних відносин та права (науковців і практиків) для наукового обгрунтування та розробки законодавчих актів у сфері суспільних інформаційних відносин та кодифікації їх норм.

3. Кабінет Міністрів України формує чи визначає провідний міжгалузевий орган центральної виконавчої влади (міжвідомчу урядову комісію), який буде відповідальним за організацію та забезпечення створення проектів законодавчих актів та кодифікації інформаційного законодавства.

4. Визначений Кабінетом Міністрів України орган центральної виконавчої влади безпосередньо створює умови та забезпечує діяльність робочої групи щодо систематизації інформаційного законодавства України.

5. Інші заінтересовані міністерства та відомства вносять свої пропозиції до організації робочої групи, у межах своїх можливостей та компетенції сприяють її діяльності.

6. Проекти нормативних актів попередньо розглядаються на спільних засіданнях Консультативної ради з питань інформатизації при Верховній Раді України, Урядової комісії з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади, інших урядових органів і представників відповідних структур міністерств, відомств та інших центральних органів виконавчої влади.

7. Проекти нормативних актів виносяться на обговорення громадськості через засоби масової інформації (пресу, радіо, телебачення тощо).

8. Пропозиції щодо удосконалення окремих положень проектів нормативних актів адресуються до створеної робочої групи.

9. Для урахування думок авторів пропозицій, їх обгрунтування організовуються та проводяться наукові конференції, семінари тощо.

10. Після розгляду пропозицій та доопрацювання проекти нормативних актів надсилаються на розгляд Верховній Раді України у порядку, визначеному для проходження законопроектів.

11. Розробки нових законів та підзаконних нормативних актів у сфері суспільних інформаційних відносин можуть поєднуватися з розробкою проекту Кодексу про інформацію.

Розділ 13. Фінансове забезпечення роботи щодо систематизації інформаційного законодавства України

1. Фінансове забезпечення роботи щодо систематизації інформаційного законодавства України здійснюється відповідно до Національної програми завдань і проектів з інформатизації та інших програм, в яких визначені проблеми суспільних інформаційних правовідносин, права інтелектуальної власності та інформаційної безпеки України.

2. Заінтересовані органи державної влади, міністерства та відомства здійснюють додаткове фінансування та матеріальне забезпечення функціонування робочої групи щодо систематизації інформаційного законодавства.

3. Фінансову підтримку робочій групі також можуть надавати недержавні організації, громадські фонди, благодійні організації у порядку, визначеному законодавством України та міждержавними угодами.

Частина 3. Тактика організації боротьби з комп'ютерною злочинністю в Україні

Розділ 14. Напрямки організаційних заходів

14.1. Напрями тактики протидії кіберзлочинності

Тактика організації протидії кіберзлочинності має такі напрями:

організаційно-управлінські;

організаційно-правові;

організаційно-інженерні (апаратно-програмні, програмно-математичні, технічні, технологічні, метрологічні, інші засоби і заходи технічного захисту інформації).

Тактика боротьби з комп'ютерною злочинністю визначається відповідно до розвитку науково-технічного прогресу, наукових досягнень у різних галузях науки, економічних, політичних умов і можливостей органів державної влади, а також правових засад у декілька етапів.

Кожний етап визначається у загальнодержавних і галузевих програмах щодо:

інформаційної та економічної безпеки, як складових національної безпеки;

боротьби зі злочинністю, у тому числі такою, що має ознаки організованої.

У зв'язку із зазначеним, Президентом та Урядом України визначені такі цільові заходи:

формування Концепції інформаційної безпеки України;

розробка Державної програми боротьби з комп'ютерною злочинністю;

розробка Концепції легалізації комп'ютерних програмних продуктів та боротьби з нелегальним їх використанням;

реалізація положень Основних напрямів боротьби з організованою злочинністю в Україні.

Орієнтовно визначаються на першому етапі створення і розвиток окремих функціональних структур по боротьбі з комп'ютерною злочинністю:

у Міністерстві внутрішніх справ України –

відділення (відділи) у складі підрозділів -

Головного управління по боротьбі з організованою злочинністю;

Головного управління Державної служби по боротьбі з економічною злочинністю;

самостійна структура на рівні відділу з перспективою формування окремого управління в МВС;

у Службі безпеки України –

в структурі контррозвідки, підрозділів боротьби з організованою злочинністю;

у Державній податковій адміністрації України –

в структурі податкової міліції.

14.2. Організація роботи з кадрами щодо протидії кіберзлочинності

Успішна протидія кіберзлочинності можлива при відповідному кадровому забезпеченні - підготовці фахівців, які спеціалізуються на розкритті злочинів, що вчиняються з використанням комп'ютерних технологій.

Підготовка кадрів має здійснюватися за такою моделлю:

у відомчих навчальних закладах правоохоронних органів (МВС, СБУ, Державній податковій адміністрації тощо) готуються спеціальні навчальні дисципліни за тематикою "Виявлення, профілактика та розкриття злочинів, що вчиняються з використанням комп'ютерних технологій".

В Національній академії внутрішніх справ України, в Національній академії служби безпеки України, в Академії державної податкової служби України (на факультеті податкової міліції) формуються на рівні магістратури спеціалізовані групи щодо підготовки викладачів для відомчих закладів освіти за проблематикою боротьби з кіберзлочинністю.

В системі закладів підвищення професійної підготовки та перепідготовки оперативного складу, слідчих та експертів проводяться спеціальні збори для навчання щодо виявлення, профілактики та розкриття комп'ютерних злочинів.

Відповідна підготовка здійснюється у системі підвищення кваліфікації підрозділів Генеральної прокуратури та суддів.

Розділ 15. Міжнародна класифікація комп'ютерних злочинів

З метою організації протидії міжнародній кіберзлочинності, а також для координації діяльності правоохоронних органів України з правоохоронними органами інших країн та міжнародними організаціями до упорядкування законодавства України щодо боротьби з комп'ютерними злочинами правоохоронні органи України здійснюють їх класифікацію, кодування та облік відповідно до рекомендацій Інтерполу, міждержавних нормативів таким чином:

QA = Втручання в роботу або перехоплення інформації у комп'ютерній системі:

QAH = Незаконний (несанкціонований) доступ до комп'ютерної системи.

QAI = Перехоплення інформації, що циркулює в комп'ютерній мережі.

QAT= Викрадення часу за надані платні послуги (наприклад, ухилення від сплати за інформаційні послуги телефонного чи комп'ютерного зв'язку в Інтернет чи переведення їх на іншого користувача подібних послуг).

QAZ = Інші випадки несанкціонованого доступу або перехоплення інформації.

QD = Зміна (модифікація) або пошкодження інформації в автоматизованій (комп'ютерній) системі:

QDL = "Логічна бомба".

QDT = "Троянський кінь".

QDV = "Комп'ютерні програми – віруси".

QDW = "Комп'ютерні програми – черв'яки"

QDZ= Інші випадки пошкодження інформації в автоматизованій системі.

QF = Комп'ютерне шахрайство:

QFC = Шахрайство з автоматами видачі готівки (банкоматами).

QFF= Комп'ютерна підробка (підроблення інформації в автоматизованій системі).

QFG = Шахрайство з комп'ютерними ігровими автоматами.

QFM = Шахрайство шляхом неправильного вводу/виводу або маніпуляції комп'ютерними програмами.

QFP = Шахрайство з платіжними електронними засобами.

QFT = Телефонне шахрайство.

QFZ = Інші випадки комп'ютерного шахрайства.

QR = Несанкціоноване копіювання комп'ютерних програмних продуктів:

QRG = Несанкціоноване тиражування комп'ютерної гри.

QRS = Несанкціоноване тиражування комп'ютерного програмного забезпечення (комп'ютерних програм).

QRT = Несанкціоноване тиражування напівпровідникової продукції (топологій, топографій інтегральних мікросхем).

QRZ = Інші випадки несанкціонованого копіювання комп'ютерної інформації.

QS = Комп'ютерний саботаж (диверсія):

QSH = Саботаж з технічного забезпечення комп'ютерної системи.

QSS = Саботаж з програмного забезпечення комп'ютерної системи.

QSZ = Інші види комп'ютерного саботажу.

QZ = Злочини, пов'язані з комп'ютерами (комп'ютерними технологіями):

QZB = Незаконне використання дошки електронних оголошень (BBS)

QZE = Викрадення комерційної таємниці.

QZS= Зберігання або розповсюдження матеріалів, які є об'єктом судового переслідування.

QZZ = Інші випадки вчинення злочинів, пов’язаних з комп’ютерами.

Розділ 16. Правова доктрина боротьби з кіберзлочинами в Україні

До узгодження Кримінального та Кримінально-процесуальних кодексів України тактика боротьби з окремими проявами кіберзлочинів здійснюється відповідно до доктрини багатооб’єктності злочинного посягання, згідно кримінального законодавства.

Кримінально-правова кваліфікація комп’ютерних злочинів здійснюється відповідно до родових та окремих безпосередніх об’єктів, визначених в особливій частині Кримінального кодексу України та положеннях Кримінально-процесуального кодексу України.

Розділ 17. Тактика правового забезпечення боротьби з комп'ютерною злочинністю в Україні

Систематизація правового забезпечення боротьби з комп'ютерною злочинністю здійснюється у складі інформаційного законодавства і передбачає три етапи:

1. Інкорпорація законодавства - визначення ієрархічної системи та структури інформаційного законодавства на рівні правової доктрини.

2. Виділення в системі законодавства галузі та закріплення її легально у Зводі законів України як розділу - "Інформаційне законодавство".

3. Кодифікація - розробка і прийняття Верховною Радою України такого нормативного акта, як Кодекс України про інформацію (далі Кодекс).

У цьому Кодексі повинні бути зведені і систематизовано узгоджені між собою та іншим законодавством України її зобов'язаннями щодо інтеграції у світове співтовариство, в тому числі відповідно до Програми інтеграції України до Європейського Союзу (розділу 13 "Інформаційне суспільство").

Розділ 18. Організаційно-правові заходи щодо державного регулювання боротьби з комп'ютерною злочинністю

Ініціювання Урядом та Президентом України:

1. Визначення у Зводі законів України як галузі законодавства (на рівні окремого розділу) – "Інформаційне законодавство".

2. Проведення систематизації національного інформаційного законодавства на рівні окремого Кодексу – "Кодексу України про інформацію" з урахуванням тенденцій розвитку інформатизації та інших суспільних інформаційних відносин.

3. Внесення змін і доповнень до кримінального, деліктного адміністративного, цивільного та трудового законодавства України:

до Кримінального кодексу України з урахуванням можливих нових проявів кіберзлочинності:

- главу III "Злочин, його види та стадії" доповнити статтею 12^1 такого змісту:

"Злочини з використанням інформаційних технологій".

“За вчинення злочинів проти основ національної безпеки, чи проти життя та здоров’я особи, чи проти волі, честі та гідності особи, чи проти виборчих та трудових та інших особистих прав і свобод людини і громадянина, чи проти власності, чи у сфері господарської діяльності, чи проти громадської безпеки, чи вчинення інших злочинів, передбачених цим Кодексом, з використанням функціональних можливостей автоматизованих комп’ютерних систем, комп’ютерних мереж, інформаційних комп’ютерних ресурсів та інших інформаційних технологій, побудованих на основі застосування сучасної обчислювальної та комунікаційної техніки покарання призначається за статтями Особливої частини, в яких передбачається відповідальність за такий злочин. При цьому робиться посилання на цю статтю”.

Такий правовий захід дозволить забезпечити здійснення організаційних та інших заходів, у тому числі об’єктивного моніторингу та статистику комп’ютерних злочинів і комп’ютерної злочинності в Україні;

у проекті нового Кодексу України про адміністративні правопорушення, у Особливій частині виділити главу “Адміністративні правопорушення у сфері суспільних інформаційних відносин і зв’язку”.

У цій главі мають знайти відображення диспозиції правопорушень, визначених у законах України “Про інформацію”, “Захист інформації в автоматизованих системах” та інших норм інформаційного законодавства України.

Для усунення протиріч та з метою однозначного тлумачення відповідних термінів і понять є необхідність узгодити на законодавчому рівні понятійний апарат щодо правопорушень, визначених в законах України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю".

Участь та ініціювання щодо розробки двосторонніх та багатосторонніх міждержавних угод щодо боротьби з комп’ютерною злочинністю.

Розробники проекту Концепції стратегії і тактики боротьби з комп'ютерною злочинністю в Україні

Кондратьєв Ярослав Юрійович - Керівник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинність при Президентові України, кандидат юридичних наук, професор, член-кореспондент Академії педагогічних наук України.

Швець Микола Якович - Керівник Центру правової інформатики Академії правових наук України, доктор економічних наук, професор, Заслужений діяч науки та техніки України.

Калюжний Ростислав Андрійович - начальник кафедри Київського Інституту внутрішніх справ при Національній академії внутрішніх справ України, доктор юридичних наук, професор.

Джужа Олександр Миколайович - начальник кафедри Національної академії внутрішніх справ України, доктор юридичних наук, професор.

Іщенко Андрій Володимирович - вчений секретар Національної академії внутрішніх справ України, доктор юридичних наук, професор.

Романюк Богдан Васильович – Перший заступник Керівника Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинність при Президентові України.

Камлик Микола Ілліч - заступник Керівника Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинність при Президентові України, кандидат економічних наук, доцент.

Гавловський Владислав Данилович - начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинність при Президентові України, кандидат юридичних наук.

Цимбалюк Віталій Степанович - провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинність при Президентові України, кандидат юридичних наук.

Хахановський Валерій Георгійович - начальник кафедри Інституту управлінням Національної академії внутрішніх справ України, кандидат юридичних наук, доцент.

Гуцалюк Михайло Васильович - старший науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з

організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинність при Президентові України, кандидат юридичних наук.

Колпак Руслан Леонідович – Служба безпеки України.

Гриценко Віталій Володимирович – начальник кафедри факультету податкової міліції Академії державної податкової служби України, кандидат юридичних наук, доцент.

Гега Петро Терентійович – начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинність при Президентові України,, кандидат юридичних наук.

Бутузов Віталій Миколайович – старший науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинність при Президентові України, кандидат юридичних наук.

Юрченко Олександр Михайлович – начальник відділу управління Державної служби по боротьбі з економічною злочинністю ГУ МВС України в м. Києві, кандидат юридичних наук.

Бєляков Костянтин Іванович – докторант Національної академії внутрішніх справ України, кандидат юридичних наук.