УДК 343.97 + 351.745.7 + 351.73 + 343.533

Бутузов Віталій Миколайович –
головний науковий співробітник МНДЦ з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук,

Гавловський Владислав Данилович –
начальник відділу МНДЦ з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук, старший науковий співробітник,

Корягін Артем Володимирович –
науковий співробітник МНДЦ з проблем боротьби з організованою злочинністю при РНБО України

Несанкціонований доступ до комп'ютерних мереж як явище і правова категорія: умови існування та організація протидії

У статті розглянуто характеристику несанкціонованого доступу до інформаційно-телекомунікаційних систем. Дано класифікацію детермінант, що впливають на існування цього негативного явища. Представлено організаційно-правові засади протидії несанкціонованому доступу до інформаційно-телекомунікаційних систем.

Інтенсивне впровадження сучасних інформаційних технологій в економіці, управлінні, кредитно-банківській діяльності, стрімкий розвиток інформаційно-телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет та спрощення доступу до неї широкого кола користувачів через персональні комп'ютери – обумовило зростання злочинних проявів у зазначеній сфері. На думку кримінологів, у тому числі міжнародних експертів, зростання злочинності у сфері високих технологій представляє дуже серйозну загрозу як для економіки, так і для інформаційної безпеки держави, складової національної безпеки. Особливо це відчувається з приєднанням до міжнародних систем телекомунікацій та підвищення інтелектуального рівня зловмисників, які через мережу Інтернет отримують доступ до комп'ютерної інформації.

У свою чергу, комп'ютерний тероризм визначено загрозою національним інтересам і безпеці в інформаційній сфері. Протиправний несанкціонований доступ є складовою у механізмі формування та реалізації загроз комп'ютерної злочинності, комп'ютерного тероризму, а також загрози розголошення інформації з обмеженим доступом (ст. 7 Закону України "Про основи національної безпеки України").

Питання організаційно-правової протидії несанкціонованому доступу до комп'ютерів, їх систем та комп'ютерних мереж в Україні висвітлювались у роботах Г.О. Андрощука, О.Ф. Величко, Б.А. Демидова, В.В. Домарева, М.В. Карчевського, П.П. Крайнєва, О.В. Потія, О.П. Скрипника, О.В. Сосніна, інших науковців та дослідників країни; у державах СНД – у роботах А.І. Дороніна, В.І. Ярочкіна та ін. У розробці положень Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" (усіх редакцій) [1], відповідних ДСТУ та НД системи

ТЗІ брали участь законодавці, науковці та співробітники Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (на сьогодні – Держспецзв'язку) та Держстандарту України. Дослідження зазначених та суміжних із ними питань в Україні на рівні загальнодержавних заходів проводили Б.А. Кормич, В.І. Гурковський, С.О. Орлов, із наведенням результатів роботи науковців у власних дисертаціях.

Стрімкий розвиток нових технологій обумовлює постійне удосконалення термінології у сфері інформаційних технологій. Зокрема, законодавець, приймаючи в Україні нову редакцію закону про захист інформації [1], у його назві замість терміну "автоматизована система" вже використовує термін "інформаційно-телекомунікаційна система". З урахуванням дії цього фактору явище несанкціонованого доступу до комп'ютерних мереж розглядається більш широко – як явище несанкціонованого доступу до інформаційно-телекомунікаційних систем.

Поширення масштабів користування мережею Інтернет при повній відсутності адміністративно-територіальних кордонів в електронному просторі і майже безконтрольності проходження інформації сприяють виникненню нових видів злочинів у цій сфері та їх високій латентності [2]. Високотехнологічні злочини набувають усе більш організованого, транснаціонального характеру. Таким чином, широке впровадження комп'ютеризованих інформаційно-телекомунікаційних систем (автоматизованих комп'ютерних інформаційних систем) на світовому рівні створює багато нових проблем, які потребують наукового дослідження і практичного вирішення.

Послуги доступу до глобальної мережі Інтернет в Україні надають більше 1600 підприємств, зокрема, 624 Інтернет-провайдери та більше 1000 Інтернет-клубів (Інтернет-кафе). Також, в українському сегменті мережі Інтернет створено 873 Інтернет-портали та 1912 Інтернет-магазинів. Кількість користувачів мережі Інтернет в Україні становить близько 4 млн. осіб. Стаціонарним телефонним зв'язком в Україні користуються більше 12,5 млн. абонентів, з яких близько 10 млн. абонентів обслуговує ВАТ "Укртелеком". Майже 1 млн. абонентів обслуговують приватні оператори зв'язку. Мережею мобільного зв'язку в Україні користуються близько 49 млн. абонентів [3].

В Україні набули поширення наступні служби переказів: служби поштових переказів Western Union – 17 банків-агентів, Money Gram – 11 банків-агентів, система банківських переказів Anelik – 52 банки-агенти.

Швидкими темпами розвиваються позабанківські електронні платіжні системи. Так, серед позабанківських систем розрахунків on-line (в режимі реального часу) самою поширеною є WebMoney. До її системи на даний час належать: пункти поповнення WM гаманців – 586, обмінних пунктів – 43, реєстраторів – 9, персоналізаторів – 25, WM дилерів – 32, точок продажу WM карт – 260, пунктів поповнення WM гаманців готівкою – 251.

На теперішній час в Україні діє 173 банки, які є членами внутрішньодержавних і міжнародних карткових платіжних систем та здійснюють емісію й еквайрінг платіжних карток.

Загальна кількість платіжних карток, емітованих українськими банками, складає 48 млн. 134 тис. шт. Банкоматів, що обслуговують платіжні картки – близько 19 тис. 350 шт., платіжних терміналів – 65 тис. 500 шт., імпринтерів – близько 33 тис. 800 шт.

Масштаби використання інформаційно-телекомунікаційних технологій, що характеризують вищезазначені цифри, та наявність невирішених проблемних питань об'єктивно обумовили криміногенний стан у цій сфері відносин.

Аналіз криміногенної ситуації свідчить, що найбільш поширеними видами злочинів в Україні у сфері інформаційно-телекомунікаційних технологій (на підставі даних за 2006 рік) є:

– несанкціоноване втручання в роботу комп'ютерних та телекомунікаційних мереж;

– несанкціонований збут та розповсюдження інформації з обмеженим доступом;

– шахрайство з використанням комп'ютерної техніки, шахрайство в мережі Інтернет, шахрайство з боку операторів зв'язку та абонентів телекомунікаційних компаній;

– підробка банківських платіжних карток [4].

Крім цього, в Україні також поширені наступні види злочинів:

– виготовлення та розповсюдження шкідливих комп'ютерних програм;

– порушення правил експлуатації комп'ютерних та телекомунікаційних мереж;

– несанкціонована зміна маршрутизації міжнародного телефонного трафіку.

Самостійним видом злочинного промислу стало викрадення ідентифікаційних даних осіб, використовуючи які злочинці отримують доступ до чужих банківських рахунків, безоплатно користуються послугами Інтернет-провайдерів та операторів зв'язку [5].

У структурі злочинів, викритих у сфері інформаційно-телекомунікаційних технологій, 26 % складають злочини у сфері комп'ютерних та Інтернет-технологій, 28 % – у сфері функціонування електронних платежів або платіжних карток, 16 % – у сфері телекомунікацій. Решта – пов'язані з використанням комп'ютерних технологій при вчиненні традиційних злочинів.

Аналіз статистики та матеріалів практики свідчить, що в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку найчастіше вчиняються злочини, які кваліфікуються за ст. 361 КК України "Несанкціоноване втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку", а саме злочини, що пов'язані з несанкціонованим втручанням в роботу комп'ютерів, автоматизованих систем та комп'ютерних мереж, що призводить до витоку, втрати, підробки, блокування інформації або спотворення процесу її обробки.

На даний час підприємства, установи та організації, а також органи державної влади та місцевого самоврядування все більше зіштовхуються з різними проявами несанкціонованих (у ряді випадків – протиправних) дій, вчинених особами з використанням інформаційно-телекомунікаційних технологій. Наслідками цих дій може бути повна або часткова функціональна бездіяльність організацій та значні матеріальні збитки.

Особами, потерпілими від реалізації протиправного несанкціонованого доступу до комп'ютерних мереж (інформаційно-телекомунікаційних систем), можуть бути:

– фізична особа, яка використовує комп'ютерну техніку за місцем проживання для власних цілей, як правило, не застосовуючи або недостатньо застосовуючи засоби програмного захисту комп'ютерної системи. Посягання зловмисників здійснюються відносно ідентифікаторів доступу до мережі Інтернет, а також відносно конфіденційної інформації даної особи;

– юридична особа, у діяльності якої використовуються інформаційні технології, зокрема для збереження інформації, яка є банківською, комерційною таємницею, електронних версій продуктів власного виробництва та послуг (у т.ч. інформаційних), а також ідентифікатори доступу до послуг мережі Інтернет або інших "віддалених сервісів" зазначеної особи;

– юридична особа (органи державної влади, установи, підприємства), інформаційна інфраструктура яких забезпечує функціонування сфер, критичних для державного управління та економіки [6].

За результатами моніторингу повідомлень ЗМІ, до найбільш резонансних актів протиправного несанкціонованого доступу слід віднести: умисні несанкціоновані дії

штатного працівника (системного адміністратора) відносно систем управління Ігналінської АЕС Республіки Литва (1993 р.) [7]; аварію з тяжкими наслідками за рахунок роботи програмного забезпечення зарубіжної розробки у системах газопостачання СРСР; блокування систем управління польотами літаків у США (11 вересня 2001 р.); керування сторонньою особою військовим супутником Великобританії (за наявної інформації причиною є часткове об'єднання систем управління військових та комерційних космічних об'єктів) тощо.

Аналіз результатів відповідних кримінологічних досліджень за кордоном [8] свідчить, що у більшості інцидентів (70–80 %) беруть участь працівники та посадові особи потерпілих організацій, що визначає загрозу протиправних несанкціонованих дій не лише як зовнішню, а також як внутрішню загрозу, а пошук шляхів її нейтралізації та подолання спрямовує на розробку та реалізацію комплексу організаційно-правових та організаційно-технічних заходів захисту інформації в інформаційно-телекомунікаційних системах.

Ефективна протидія протиправному несанкціонованому доступу до інформаційно-телекомунікаційних систем потребує з'ясування переліку причин чинників, які впливають на умови його існування. Ці чинники можна поділити на політико-правові, економічні, організаційно-технічні, соціально-психологічні та криміногенні.

До політико-правових чинників слід віднести:

– відставання правових норм від науково-технічного прогресу та розвитку нових технологій зокрема;

– відсутність Концепції (Доктрини) інформаційної безпеки України.

До економічних:

– пріоритетність інтересів капіталу щодо найшвидшого отримання прибутку, підвищення рентабельності, у т.ч. за рахунок економії на витратних технологіях захисту інформаційно-телекомунікаційних мереж;

– залежність економічних процесів від організації інформаційно-телекомунікаційних систем.

До організаційно-технічних:

– складність автоматичного та автоматизованого системного відстеження всієї сукупності взаємозв'язків у роботі інформаційно-телекомунікаційної системи, забезпечення безпеки обробки та передачі даних у них;

– проблеми ідентифікації в інформаційно-телекомунікаційних системах особи користувача (інших повноважних суб'єктів) та аутентифікації їх дій з інформаційними ресурсами;

– обмеженість суто технічних рішень забезпечення інформаційної безпеки за відсутності концептуального підходу та врахування "людського фактору" під час їх впровадження та експлуатації.

До криміногенних:

– правоохоронцям складно окреслити території, на яких здійснюються сучасні злочини, комп'ютерна злочинність вже давно стала транснаціональною;

– у злочинців у мережі Інтернет великий ступінь анонімності, а інформація, що зберігається в комп'ютерних системах, має короткостроковий характер.

Соціально-психологічний чинник – формування та існування в суспільстві позитивного образу порушника ("хакера", "кардера" тощо), який може більш-менш вільно отримувати протиправні прибутки.

Існування загрози протиправного несанкціонованого доступу до комп'ютерних мереж (інформаційно-телекомунікаційних систем) в Україні та у світі потребує визначення та протидії цьому негативному явищу, зокрема у правовому полі.

У широкому розумінні, як правова категорія, *несанкціонований доступ до інформаційно-телекомунікаційних систем – це сукупність різних за характером суспільної небезпеки, але єдиних за своєю суттю діянь (кримінальних,*

адміністративних, цивільно-правових, господарсько-правових, дисциплінарних) з питань володіння, користування, розпорядження та захисту інформації (яка зберігається, обробляється та передається за допомогою інформаційно-телекомунікаційних систем, а охорона прав та законних інтересів відносно якої передбачена законодавством України), визначених у відповідних статтях кодексів та законів України, підзаконних нормативно-правових актах, а також в угодах між суб'єктами господарювання, трудовими колективами та окремими працівниками.

Протиправний несанкціонований доступ до інформаційно-телекомунікаційних систем, як кримінально-правова категорія, має такі особливості:

1) лише частина дій осіб, які утворюють явище несанкціонованого доступу, мають ознаки "деліктності" й, відповідно, передбачають адміністративну або кримінальну відповідальність винних осіб (ст. 1 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", п.п. 5.5, 5.6, 5.11 ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення.");

2) несанкціонований доступ у якості способу вчинення практично присутній в усіх складах злочинів, передбачених статтями 361, 361-1, 361-2, 362, 363, 363-1 Розділу XVI КК України "Злочини у сфері використання комп'ютерів, їх систем та комп'ютерних мереж і мереж електрозв'язку";

3) несанкціонований доступ до комп'ютерних мереж, як спосіб вчинення злочинів, присутній в інших статтях різних розділів КК України. Як обов'язковий, він передбачений у складах злочинів за ст.ст. 163 та 359 КК України, а як факультативний – присутній у ст.ст. 114, 182, 200, 231, 232, 232-1, 328, 330, 359 та в інших статтях КК України.

Тому, розглядаючи його як кримінально-правову, криміналістичну та кримінологічну категорію, необхідно обмежуватись лише колом "деліктного" несанкціонованого доступу до комп'ютерних мереж (інформаційно-телекомунікаційних систем).

"Деліктний" несанкціонований доступ до інформаційно-телекомунікаційних систем – це сукупність злочинів та адміністративно-правових деліктів, які полягають у порушенні конфіденційності, цілісності, доступності, витоку інформації (у т.ч. інформації з обмеженим доступом), що зберігається, передається та обробляється в інформаційно-телекомунікаційних системах, права та законні інтереси відносно якої охороняються Кримінальним кодексом України й Кодексом України про адміністративні правопорушення, або у створенні реальної загрози цього.

Протиправний несанкціонований доступ створює наступні загрози національним інтересам і безпеці в інформаційній сфері: комп'ютерна злочинність та комп'ютерний тероризм, розголошення державної таємниці та іншої інформації, охорона якої визначена державою для захисту зазначених інтересів. З метою протидії загрозі протиправному несанкціонованому доступу, який є складовим у загрозах національній безпеці в інформаційній сфері та в інших сферах життєдіяльності суспільства України, діяльність державних органів та їх підрозділів повинна спрямовуватись на протидію всім загрозам, визначеним розгорнутим переліком загроз інформаційній безпеці України.

Розгорнутий перелік загроз має бути визначений у Концепції інформаційної безпеки України, але Концепція на даний час відсутня.

Існують загальні загрози інформаційній безпеці, а також її специфічні загрози у сферах оборони, економіки, під час надзвичайних ситуацій [9; 10; 11] тощо. У зв'язку з цим утворюється розмаїття загроз та відповідних напрямів протидії.

Зовнішній вияв сукупності цієї діяльності є формою протидії певній загрозі, обмеженою компетенцією органів, задіяних у процесі протидії, та об'єктивними факторами прояву загрози. У залежності від сфери суспільних відносин та конкретної загрози, форма протидії має загальні та специфічні ознаки, а у

конкретному випадку прояву загрози – конкретні ознаки протидії у вигляді заходів, здійснюваних підрозділами організаційних структур за компетенцією, окремих дій їх працівників та інших осіб, відповідно до їх прав та обов'язків, визначених чинним законодавством України.

За результатами дослідження до проекту Інформаційного кодексу України нами пропонуються наступні визначення:

1. Форма протидії несанкціонованому доступу до комп'ютерних мереж (інформаційно-телекомунікаційних систем) – організована діяльність відповідних підрозділів державних органів, недержавних організацій або окремих громадян, здійснювана на різних напрямах у межах компетенції та відповідно до завдань, визначених законами, підзаконними нормативно-правовими актами та угодами, що реалізується у заходах протидії на етапах попередження, виявлення, припинення, розслідування фактів протиправних несанкціонованих дій, вчинених (у т.ч. з використанням інформаційно-телекомунікаційних систем) відносно інформації, створеної та захищеної відповідно до законодавства України, та нейтралізації їх наслідків.

2. Засоби протидії несанкціонованому доступу до комп'ютерних мереж (інформаційно-телекомунікаційних систем) – сукупність організаційно-правових та організаційно-технічних заходів, спрямованих на виявлення, припинення, документування та оцінювання дій, які мають ознаки несанкціонованих та (або) протиправних, та безпосередньо пов'язані з порушенням конфіденційності, цілісності, доступності інформації, створеної та захищеної згідно законодавства України.

Зокрема, охорона державної таємниці як комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв (ст. 1 Закону України "Про державну таємницю") є прикладом значної за обсягом заходів та загальною формою протидії несанкціонованому доступу до державної таємниці, у т.ч. вчиненого за допомогою комп'ютерних мереж.

У вищенаведеному ДСТУ 3396.2-97 визначено, що систему технічного захисту інформації, у сукупності з матеріально-технічною базою, також утворюють організаційні структури й нормативно-правові документи. Вищезазначене дає підстави для висновку, що до окремих елементів системи забезпечення інформаційної безпеки в Україні, крім технічних засобів та іншого матеріально-технічного забезпечення, слід віднести компетентні організаційні структури (підрозділи) та нормативно-правові акти, якими врегульовано їх діяльність.

Аналіз норм Закону України "Про основи національної безпеки України", а саме: положення про необхідність формування та реалізації заходів державної політики, дозволяє зробити припущення, що формами протидії слід вважати як первинний етап в організації діяльності компетентних органів щодо забезпечення інформаційної безпеки, так й процес її поточної реалізації, у т.ч. взаємодію з іншими елементами системи для досягнення її загальної мети – захищеності національних інтересів. Взаємодію державних органів України, як організацію та процес спільної діяльності їх підрозділів, зокрема на рівні міжвідомчої та міждержавної взаємодії, також пропонується розглядати у якості форм протидії протиправному несанкціонованому доступу.

На підставі вищенаведеного слід визначити, що найбільш проблемними питаннями боротьби з таким видом злочинності на сьогодні залишаються:

1. Приведення національного законодавства у відповідність вимогам Конвенції ООН проти транснаціональної організованої злочинності та Конвенції про кіберзлочинність, подальше вдосконалення нормативно-правової бази, яка регулює боротьбу зі злочинністю у сфері комп'ютерних технологій (розширення можливостей національних правоохоронних органів з урахуванням

транснаціонального характеру комп'ютерної злочинності, розроблення ефективного механізму взаємодії національних правоохоронних органів з компетентними органами інших країн).

2. Відсутність ефективної правової допомоги щодо перевірки заяв та повідомлень про злочинні дії, коли потерпілий або злочинець знаходяться в іншій країні. Для цього необхідно створення національного контактного центру по боротьбі з комп'ютерною злочинністю, який здійснював би координацію діяльності оперативних та слідчих підрозділів правоохоронних органів із закордонними правоохоронними органами.

3. Викриття та розслідування злочинів, пов'язаних з несанкціонованим втручанням до інформаційно-телекомунікаційних систем, обумовлює використання правоохоронними органами певних технічних та програмних засобів для пошуку та фіксації фактичних даних про протиправні діяння у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку. Тому, необхідне відповідне матеріально-технічне забезпечення вузькоспеціалізованих підрозділів по боротьбі з комп'ютерною злочинністю, здатних застосовувати сучасні методи оперативно-технічного документування злочинів даного виду. Наприклад, фіксація фактів несанкціонованого втручання у роботу мереж електрозв'язку та порушень встановленого порядку маршрутизації міжміського та міжнародного телефонного трафіку неможлива без застосування спеціального обладнання (наприклад, аналізатора сигналізації телекомунікаційних систем (АСТС)), та залучення до проведення перевірок спеціально підготовлених фахівців у галузі телекомунікацій. Крім того, виникають проблеми з обрахуванням матеріальної шкоди, що завдається правопорушниками при втручанні в роботу мереж електрозв'язку операторів міжнародного зв'язку, які відмовляються надавати відповідну інформацію правоохоронним органам, посилаючись на відсутність єдиної методики обрахування збитків.

4. Низький рівень інформаційного забезпечення правоохоронних органів про реальний стан злочинності в інформаційно-телекомунікаційній сфері, високий рівень латентності кіберзлочинності. Так, залишається невирішеною проблема достатнього аналітично-методичного забезпечення протидії правопорушенням у сфері високих технологій: встановлення та прогнозування нових криміногенних загроз та проявів, пов'язаних з недосконалістю законодавства і впровадження в економіку новітніх технологій, розроблення ефективних методів оперативного документування високотехнологічних злочинів, аналізу криміногенної ситуації на ринку послуг використання новітніх технологій.

На підставі проведеного аналізу проблемних питань протидії негативним тенденціям щодо поширення протиправних дій, пов'язаних з несанкціонованим доступом до комп'ютерних мереж та проявами комп'ютерного тероризму, пропонуються наступні шляхи їх вирішення в Україні:

1. Приведення національного законодавства у відповідність вимогам сьогодення, подальше вдосконалення нормативно-правової бази, яка регулює боротьбу зі злочинністю у сфері інформаційно-телекомунікаційних технологій.

2. Створення структури з відповідними функціями та повноваженнями у сфері боротьби з високотехнологічною злочинністю, у т.ч. спеціалізованого підрозділу, виключною компетенцією якого стала б боротьба зі злочинністю у сфері інформаційно-телекомунікаційних технологій, за умови залучення відповідних ресурсів, сприятиме підвищенню ефективності роботи правоохоронної системи України.

3. Налагодження ефективної взаємодії з міжбанківськими інституціями, телекомунікаційними компаніями, зацікавленими центральними державними

органами та правоохоронними органами інших країн з метою документування злочинних груп з міжнародними зв'язками.

4. Відповідне методичне та матеріально-технічне забезпечення національних правоохоронних структур для ефективної боротьби з високотехнологічною злочинністю.

Список використаних джерел

1. *Закон* України № 80/94-вр (в редакції Закону № 2594-IV від 31.05.2005 р.) "Про захист інформації в інформаційно-телекомунікаційних системах" <http://www.rada.gov.ua>, 11 жовтня 2007 р.

2. *Комп'ютерна* злочинність: Навчальний посібник / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. – К.: Атіка, 2002. – 240 с.

3. *Стан* та розвиток зв'язку в Україні за 2006 рік. Статистичний бюлетень / Державний комітет статистики України – Київ, 2007. – 35 с.

4. *Крамаренко М.* Как ограбить Интеренет: Украина поможет <http://sngnews.ru//frame_article/6/71648.html >, 11 жовтня 2007 р.

5. *Сапсай В.Д., Бутузов В.М., Корягін А.В.* Аналітичний огляд протидії комп'ютерної злочинності в Україні у 2003 році (за результатами діяльності підрозділів ДСБЕЗ) / За ред. В.В. Шапоренко. – К.: Департамент ДСБЕЗ МВС України. – 2004. – 35 с.

6. *Корягин А.В.* Вопросы международного сотрудничества в борьбе с компьютерной преступностью в Европе. Пути решения проблем эффективного реагирования на трансграничные преступные деяния относительно компьютерной информации // Сб. научных работ "Компьютерная преступность и кибертерроризм" по Программе малых грантов Центра по изучению транснациональной организованной преступности и коррупции при Американском университете (г. Вашингтон). – Запорожье: Центр исследования компьютерной преступности. – 2004. – 165 с.

7. *Информационное* агентство "Интерефакс-Запад". В Совете Безопасности РФ говорят об угрозе взаимосвязи ядерного терроризма и кибертерроризма (цитаты из доклада зам. секретаря Совета Безопасности РФ В. Соболева на II Международной конференции "Терроризм та электроннонные СМИ") <http://www.interfax.by/? id=33&id_sp=28411>, 11 жовтня 2007 р.

8. *Айков Д., Сейнер К., Фонсторх У.* Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. – М.: Мир, 1999. – 351.

9. *Закон* України від 04.02.1998 р. № 75/98-ВР "Про Концепцію Національної програми інформатизації" <http://www.rada.gov.ua>, 11 жовтня 2007 р.

10. *Доктрина* информационной безопасности Российской Федерации, утверждена Президентом РФ № Пр-1895 от 09.09.2000 г. <http://www.scrf.gov.ru/ documents/5.html>, 11 жовтня 2007 р.

11. *Концепция* информационной безопасности Республики Казахстан, одобренная Указом Президента Республики Казахстан от 10.10.2006 г. № 199 <http://www.minjust.kz/>, 11 жовтня 2007 р.

The article is devoted to the characteristic of unauthorized access to the informational-telecommunication systems. The authors give the classification of the determinants exerting influence upon the existence of this negative phenomenon and represent the organization-legal bases of counteraction unauthorized access to the informational-telecommunication systems.