Правове забезпечення

УДК 343.346.8:004.056.53

В.М. Струков

Харківський національний університет внутрішніх справ

ДО ВИЗНАЧЕННЯ НАПРЯМІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Стаття присвячена аналізу причин поширення кіберзлочинності в Україні і вироблення концептуальних шляхів запобігання та протидії цьому негативному соціальне явище. Досліджено та проаналізовано коріння таких причин, як неврегульованість доступу до кіберпростору і послуг в ньому, техніко-технологічні особливості організації кіберпростору і недосконалість законодавчої бази. В результаті проведеного дослідження обґрунтовано концептуальні шляхи протидії кіберзлочинності.

Ключові слова: *інформаційна безпека, Інтернет, операційна система, комунікаційне обладнання, віртуальні відносини, сайт, кіберзлочин, профілактика.*

Вступ

Однією з найхарактерніших рис сьогодення є стрімкий рост кількості учасників відношень у кіберпросторі. За даними ООН у 2012 році число людей, що мають можливість регулярно користуватися Інтернетом, було оцінено в 2,3 мільярда. Загальна кількість власників мобільних телефонів та смартфонів зросла до 6 мільярдів.

За даними компанії Skype кількість користувачів однойменної популярної мережевої програми у 2012 році щомісяця зростала приблизно на 100 000. Цей факт красномовно підтверджує думку багатьох експертів про те, що нині людство стрімко переходить із сфери матеріальних відношень у сферу віртуальних відношень у кіберпросторі. Ця тенденція обумовлена революційними технологічними новаціями в галузі інформаційних комунікацій. І ці процеси відбуваються настільки швидко і навіть лавиноподібно, що інші галузі не встигають адекватно і своєчасно реагувати на них. До таких галузей, в першу чергу, можна віднести освіту, законотворчу і правоохоронну діяльність. Так, за даними правоохоронних органів, прибутки кіберзлочинців вже у 2011 році перевищили прибутки наркоділків і торгівців зброєю разом узятими.

Враховуючи вищенаведені темпи зростання кількості учасників відносин у кіберпросторі є очевидним подальше нарощування кількості правопорушень у кіберпросторі і проблем, пов'язаних з ними.

Основними причинами цього негативного суспільного явища є на наш погляд наступні:

1. Неврегульованість доступності кіберпростору і послуг в ньому.
2. Техніко-технологічні особливості організації кіберпростору.
3. Недосконалість нормативної бази.

Доступність кіберпростору і послуг в ньому

Доступність Інтернету регулюється такими чинниками, як:

- технологічна можливість;
- рівень економічного розвитку регіону;
- юридична можливість.

Під **технологічною можливістю** розуміється наявність відповідного технічного та програмного забезпечення, інфраструктури та провайдера – юридичної особи, яка надає послуги Інтернету. На сьогодні, враховуючі географію присутності представників розробників мережевого технічного і програмного забезпечення, а також поширення безпровідних технологій інформаційних комунікацій, можна говорити про те, що в будь-якій країні світу існує технологічна можливість доступу до Інтернету.

Разом з тим, очевидним є той факт, що не кожна людина має фінансові можливості придбання відповідної техніки, програмного забезпечення та послуг Інтернету. З цієї точки зору важливим є співвідношення цін на техніку і послуги із заробітками населення. Таким чином, доступність Мережі визначається і рівнем економічного розвитку регіону або країни. Так, близько 70 відсотків від усіх користувачів Інтернету припадає на забезпечені регіони. Вони підключені по виділених лініях за невисоку абонентську плату. Приблизно 6 відсотків проживають у регіонах із середнім рівнем економічного розвитку і витрачають на Інтернет відчутну частину свого доходу. Що залишилися 24 відсотки складають жителі бідних країн, і саме вони платять за Інтернет найбільше [12].

В Африці ціни на доступ в Інтернет перевищують американські розцінки в 7 разів і в 20 разів – європейські. Аналогічна ситуація спостерігається і в сфері послуг мобільного зв'язку.

За останніми оцінками, загальний дохід від телекомунікаційного сектора перевищує півтора трильйона доларів на рік, що становить 2,4 відсотка від валового внутрішнього продукту в світі [12].

Доступ до Інтернету вдома мають 32% дорослого населення світу. Про це свідчить останнє опитування соціологічного центру Gallup Organisation.

Для порівняння в 2010 році кількість користувачів Інтернету складала 29%, а в 2009 році – 25%.

У той же час, менше ніж одна людина з десяти в 41 країні світу має Інтернет вдома. При цьому Інтернетом вдома користуються менше 1% респондентів в Бурунді, Гвінеї, Малі та Мадагаскарі і 1% в Нігері, Камбоджі і Руанді [13].

Найбільший відсоток підключених до домашнього Інтернету – серед багатих громадян країн Європи, Азії та Північної Америки. До таких країн зокрема належать Швеція (93%), Сінгапур (93%), Данія (92%), Нідерланди (91%), Нова Зеландія (89%), Австралія (89%), Канада (87%), Тайвань (87%), Ірландія (87%), Південна Корея (87%) [13].

В Україні 40% опитаних заявили, що мають вдома доступ до Інтернету. В той же час в Угорщині ця частка становить 66%, в Росії – 51%, в Білорусі – 50%, в Румунії – 49%, Молдові – 42%, Казахстані 33%, в Грузії – 29%, в Азербайджані – 15% , в Узбекистані – 10%, а в Таджикистані – 4% [13].

Під **юридичною можливістю** будемо розуміти наявність законних підстав для придбання відповідного програмного забезпечення і доступу до послуг Мережі. Дію цього чинника в деяких державах можна проілюструвати наступними даними.

У Китаї діє так звана «Велика китайська інформаційна стіна» (Great_Firewall_of_China), яка блокує IP-адреси веб-сайтів «сумнівного змісту». У громадських інтернет-кафе люди повинні здати посвідчення особи перед тим, як сісти за комп'ютер[3].

Показовим є блокування сайту «Google», скасоване лише у січні 2006 року. Однак, згідно з домовленостями з китайським урядом, результати пошуків для китайських користувачів будуть «дещо обмежені». Заборонена у Китаї і Вікіпедія. Китайський уряд зробив це під приводом «боротьби з пропагандою насильства» [3].

У липні 2011 р. китайським урядом було видано нові постанови, які вимагають від кафе, пабів, книгарень та готелів Пекіну встановити програмне забезпечення – для відстеження дій відвідувачів, які вирішили скористатися WiFi-інтернетом. У разі невиконання цих вимог обумовлено штраф у $2,300 або позбавлення ліцензії на ведення бізнесу. Крім закриття більше, ніж мільйону порнографічних сайтів, під повною або частковою забороною опинилося декілька надзвичайно популярних ресурсів – зокрема соціальна мережа Facebook, сервіс мікроблогів Twitter та відеохостинг YouTube [3].

Незважаючи на наявність каналу зв'язку з Інтернетом, Північна Корея не має на своїй території доступних серверів Інтернету; декілька веб-сайтів, що належать північнокорейському урядові, фізично перебувають за межами країни. Тим не менш, з 2004 року в КНДР працює електронна пошта, доступна обмеженому колу осіб. Водночас на території країни діє не зв'язана з Інтернетом власна комп'ютерна мережа «Кванмен» [3].

На Кубі Всесвітньою павутиною можуть користуватись лише лікарі; іншим громадянам країни це заборонено на законодавчому рівні[3].

Починаючи з 3 грудня 2006 року для користувачів Ірану було закрито доступ до низки сайтів, серед яких Вікіпедія, YouTube, IMDb. Вважається. що це пов'язано з розгорнутою в країні кампанією боротьби зі згубним впливом західної культури. У вересні 2012 Іран вийшов із Всесвітнього павутиння, замінивши його Інтранетом [3].

29 листопада 2012 року уряд Сирії повністю відключив країну від Інтернету.

На локальному рівні також існують обмеження доступу до Мережі. Зокрема, в локальних і корпоративних мережах деяких компаній блокується доступ до ресурсів, які не пов'язані безпосередньо з роботою – різні форуми, особиста пошта, розважальні сайти та сервіси.

Таким чином, з вищенаведеного виходить, що на сьогодні, не зважаючи на відсутність електронних кордонів в Мережі, існують обмеження доступу до Інтернет на рівнях від державного до рівня окремих компаній, причому ці обмеження далеко не завжди підкріплені юридично. Спектр таких обмежень сягає від блокування окремих ресурсів до повного відключення від Мережі.

Техніко-технологічні особливості організації кіберпростору в контексті інформаційної безпеки

Під техніко-технологічними особливостями організації кіберпростору будемо розуміти ті властивості комп'ютерної техніки, комунікаційного обладнання та програмного забезпечення, які характеризують степінь захищеності інформаційної системи від зовнішнього несанкціонованого втручання. З огляду на обмежений обсяг роботи зупинимося на деяких критичних з точки зору інформаційної безпеки властивостях операційних систем та мережевого комунікаційного обладнання. Сьогодні в середовищі фахівців йдуть дискусії стосовно стратегічних напрямів подальшого розвитку операційних систем з огляду їх захищеності. Слід зауважити, що з самого початку виникнення комп'ютерної техніки і комп'ютерних мереж превалюючим напрямом всіх технологічних новацій у цій сфері було досягнення все більшої швидкості обробки і передачі інформа-

ції на різних ієрархічних рівнях з метою спрощення процедур обміну і підвищення їх ергономічної привабливості. Тому спочатку головним принципом при розробці операційних систем був принцип відкритості.

Перші операційні системи (ОС) для персональних комп'ютерів (MS-DOS і Windows версій до 3.1 включно) зовсім не мали власних засобів захисту. Більше того, системні ресурси цих ОС (системні області на жорстких дисках, вектор переривань, системна оперативна пам'ять, сегменти коду і даних програм) були абсолютно незахищені від втручання користувача, на відміну від операційних систем таких мейнфреймів, наприклад, як IBM 360/370. По-перше, це обумовило широке розповсюдження і різноманіття комп'ютерних вірусів, і, по-друге, спричинило проблему створення додаткових засобів захисту. Актуальність цієї проблеми практично не зменшилася з появою більш потужних ОС з розвиненими підсистемами захисту. Це обумовлено тим, що більшість систем не здатні захистити дані, що знаходяться за її межами, наприклад, при використанні мережевого інформаційного обміну.

На поточний момент головним напрямом розвитку операційних систем є модифікація раніше створених з метою їх адаптації до сучасних технологічних новацій і вимог (зокрема, вимог до інформаційної безпеки). Це стосується, в першу чергу, таких груп ОС як Windows та Unix. Найчастіше для проникнення в роботу цих систем хакери використовують приховані помилки в ядрі і драйверах ОС. Згідно з дослідженням університету Карнегі-Меллона, кількість помилок у військовому і промисловому програмному забезпеченні складає в середньому від п'яти до десяти на 1000 рядків коду. Мається на увазі ПЗ, що використовується на практиці і пройшло стадії тестування і впровадження. Враховуючи, що ядро операційної системи Windows містить більше 5 мільйонів рядків коду, а ядро Linux – 3,5 мільйона, неважко підрахувати кількість теоретично можливих недоліків, які можуть застосовуватися для здійснення кібератак. Тому історично склалося так, що виробники комп'ютерної та комунікаційної техніки а також програмного забезпечення зосереджувались на стабільності і відмовостійкості своїх рішень. До недавнього часу такий підхід був, безумовно, виправданий, однак зараз настав час серйозно звернути увагу на забезпечення саме інформаційної безпеки, залучаючи для співпраці і експертизи своїх продуктів спеціалізовані компанії [11].

Таким чином, світ опинився в ситуації, коли, з одного боку, деякі країни вже мають кіберзброю, а з іншого – ключові інформаційні системи держав відкриті для нападу. Залежно від рівня розвитку інформаційних технологій в країні і ступеня автоматизації конкретного промислового об'єкта атакувати його може бути простіше або складніше, але кібератака можлива.

Виходячи з цих обставин інша група експертів, зокрема, фахівці компанії «Лабораторія Касперського» пропонують іншій напрям розвитку захищених операційних систем – створення принципово нових ОС, які задовольняють вимогам надійності і захищеності функціонування. З їх точки зору така операційна система повинна відповідати наступним вимогам [11]:

• ОС не може бути заснована на якомусь вже існуючому програмному коді, тому повинна бути написана з нуля;

• з метою гарантії безпеки вона не повинна містити помилок і вразливостей в ядрі, контролюючому інші модулі системи. Як наслідок, ядро має бути верифіковано засобами, що не допускають існування вразливостей і коду подвійного призначення;

• з тієї ж причини ядро має містити критичний мінімум коду, а значить, максимальне можлива кількість коду, включаючи драйвери, має контролюватися ядром і виконуватися з низьким рівнем привілеїв;

• в такому середовищі повинна бути потужна і надійна система захисту, що підтримує різні моделі безпеки.

Додамо, що така операційна система повинна бути максимально сумісною з певною групою операційних систем, наприклад, з ОС групи Windows, для забезпечення мобільності або, в крайньому випадку, мінімальних витрат на конвертацію застосувань, що вже функціонують. В іншому випадку такий проект буде приречений на комерційний провал. Прикладом подібної ОС може слугувати операційна система «ФЕБОС», розроблена компанією «НеоБИТ» [4].

Іншим слабким місцем мережевих комунікацій є незахищеність комунікаційного обладнання, зокрема, маршрутизаторів і шлюзів і відповідного програмного забезпечення, які реалізують передачу даних за домінуючим в Інтернеті принципом комутації пакетів. Існуючі пристрої допускають модифікацію пакетів даних у проміжних точках маршруту пересування. Причому модифікації зазнають такі принципово важливі елементи пакетів як MAC-адреси і IP-адреси, що суттєво утруднює пошук джерел протиправних дій. Усунення цих причин потребує розробки нових комунікаційних пристроїв і протоколів, які б унеможливлювали несанкціоноване втручання до пакетів даних в процесі їх пересування від джерела до приймача.

Недосконалість нормативної бази

Як і в сфері матеріальних відносин у кіберпросторі не може бути вседозволеності – має бути певний баланс між тим, що можна вчиняти і тим, чого не

можна. І цей баланс повинен визначатися ступенем соціальної небезпеки того чи іншого віртуального вчинку. Зараз триває процес формування норм поведінки у віртуальному просторі. Цей процес супроводжується боротьбою між прихильниками безперешкодного поширення інформації в Інтернет і прихильниками певних обмежень дій у кіберпросторі. Перші мотивують свою позицію боротьбою за права людини, хоча це не завжди так (часто за подібними лозунгами стоять матеріальні інтереси конкретних осіб і організацій), а їхні опоненти – соціальною небезпекою, яку несе в собі абсолютна відкритість Інтернету. З цієї точки зору зрозуміла позиція власника компанії Google Сергія Бріна. В інтерв'ю британській газеті Guardian він заявив, що загроза для свободи Інтернету виходить з боку урядів, які все більш активно намагаються "систематизувати" для своїх громадян доступ до електронних засобів зв'язку і посилюють заходи контролю за їх комунікаційним обміном. Свій внесок у ці зусилля, як зазначив Брін, вносять і представники індустрії розваг, які борються з піратством. Нарешті, на його думку, свої правила нав'язують соціальні мережі, так само як і компанії - виробники програмного забезпечення[10].У числі країн, найбільш активно намагаються обмежити доступ своїх громадян в Інтернет, Брін назвав Китай, Саудівську Аравію та Іран. Серед компаній і соціальних мереж, що фактично диктують свою волю користувачам за допомогою своїх власних програмних "платформ", він відмітив Apple і Facebook.

На поточний момент у світі в різних країнах існує весь спектр норм поведінки у кіберпросторі – від практично абсолютної свободи до практично повної заборони. Причому в цій галузі вже задіяні регуляторні механізми практично всіх адміністративних рівнів – від керівництва окремої компанії до організації об'єднаних націй включно. Законодавство в сфері боротьби з кіберзлочинністю в різних країнах також ще недосконале оскільки ще не повністю врегульовані на законодавчому рівні самі віртуальні відносини.

Гострота проблеми і необхідність координації зусиль міжнародного співтовариства у сфері протидії кіберзлочинності відображена, зокрема, в «Конвенції про кіберзлочинність», яка підписана членами Ради Європи та іншими державами у 2001 році і ратифікована Законом України «Про ратифікацію Конвенції про кіберзлочинність» N 2824-IV від 07.09.2005р. Конвенція містить 48 статей, згрупованих у чотирьох розділах, які, як передбачено, повинні складати базу національного законодавства у сфері боротьби з кіберзлочинністю для держав, що підписали і ратифікували її. Але, не зважаючи на це, до сьогоднішнього дня в Україні відсутній повноцінний комплекс законодавчих актів у сфері профілактики і боротьби з кіберзлочинністю.

На даний час в Україні не існує жодного закону, який би говорив, що сайти повинні певним чином реєструватися, а також не визначений правовий статус інтернет-сайтів. У Росії, якщо на сайт "заходить" у день більш як 3 тисячі відвідувачів, він повинен реєструватися як електронний засіб масової інформації. В нас такої вимоги поки що немає.

Нещодавно міністр МВС України Віталій Захарченко виступив з ініціативою "відрегулювати" можливість доступу до інформації в Інтернеті. Він вважає, що в Мережі "дуже багато різної інформації, до якої частина населення, наприклад підлітки, взагалі не повинні мати можливості доступу".

Зі слів очільника української міліції, організатори теракту в Дніпропетровську саме з Інтернету взяли інформацію про те, як змайструвати вибухівку. На його думку, якби не всесвітня павутина, то дніпропетровські терористи ніяким іншим чином не здобули б таких знань. А отже, міністр пропонує на законодавчому рівні врегулювати доступ до Інтернету. До речі, в Росії прийнятий і діє Федеральний закон «Про захист дітей від інформації, що завдає шкоди їх здоров'ю та розвитку», а в липні 2012 року закон про заборонні поправки до законів «Про інформацію», «Про захист дітей» і «Про зв'язок». Поправки передбачають створення Єдиного державного реєстру, в який будуть вноситися доменні імена або універсальні покажчики веб сторінок, а також мережеві адреси сайтів з інформацією, забороненою до розповсюдження в Росії. Тобто, в першу чергу, це дитяча порнографія, пропаганда наркотиків і психотропних речовин, а також інформація, що спонукає дітей до самогубства (точніше, що описує, як вчинити самогубство)[9].

ТСН.ua провів власне дослідження серед користувачів соціальної мережі Facebook, у якому запитав, до якої інформації в Інтернеті варто обмежити доступ. Найбільше "юзери" соцмережі пропонували заборонити демонстрацію сцен жорсткості та насильства. Вдвічі менше противників порнографії, та приблизно стільки ж хотіли б заборонити доступ до інформації про те, як зробити бомбу.

Проблема відсутності дієвого законодавства в сфері регулювання віртуальних відносин ускладнюється ще й темпами зростання кількості кіберзлочинів і матеріальних витрат, які вони спричиняють. Так за даними МВС в 2004 році прибуток кіберзлочинців складав $104 млрд., а в 2009 році – близько $1 трлн, і по прибутковості кіберзлочинність "перевищує доходи від торгівлі наркотиками і зброєю разом узятими" [7].

І поки законотворчий процес буксує, правоохоронні органи (управління боротьби з кіберзлочинністю) мають серйозні проблеми з розслідуванням кіберзлочинів і доведенням їх до суду, а матеріальні втрати від кіберзлочинів стрімко зростають.

Висновки

Вищенаведений аналіз дає підстави зробити висновок про те, що проблема протидії і боротьби з кіберзлочинністю є багатогранною і лежить не тільки у законодавчій сфері, а і в технічній і технологічній.

Таким чином, основними стратегічними напрямами профілактики і протидії кіберзлочинності з метою гармонізації віртуальних відношень у кіберпросторі можна вважати наступні:

1. Розробка законодавчої бази, яка б регулювала відношення у кіберпросторі (профілактику кіберзлочинів, протидію і боротьбу з правопорушеннями в інформаційній сфері в тому числі). Така база може мати форму окремого кодекса або, як мінімум, окремих розділів у вже існуючих кодексах і законах. В першу чергу це стосується таких законодавчих документів як «Кримінально-прпоцесуальний кодекс», «Закон про оперативно-розшукову діяльність» та низки діючих законів, що регулюють відношення в інформаційній сфері.

2. В техніко-технологічній сфері:

– створення принципово нових ОС, які задовольняють вимогам надійності і захищеності функціонування, паралельно з модернізацією діючих ОС;

– розробка нових комунікаційних пристроїв і протоколів, які б унеможливлювали несанкціоноване втручання до пакетів даних в процесі їх пересування від джерела до приймача.

3. Створення механізму правової освіти населення щодо правил поведінки і законодавства у кіберсфері.

4. Створення системи підготовки кваліфікованих кадрів у сфері профілактики, протидії і боротьби з кіберзлочинністю.

Список літератури

1. Тихомиров О.О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки / О.О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф., (Київ, 22 берез. 2011 р.). – Ч2. – К.: Вид-во НА СБ України, 2011. – С. 78-82.

2. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 року № 514/2009 [Електрон. ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009.

3. Інтернет. [Електрон. ресурс]. – Режим доступу http://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82.

4. Защищенная операционная система «Фебос». [Електрон. ресурс]. – Режим доступу: http://www.neobit.ru/development/about-febos.html.

5. Kaspersky Security Network [Електрон. ресурс]. – Режим доступу: http://www. kaspersky.ru/ downloads/pdf/ kaspersky_security_network.pdf.

6. "Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування". Аналітична записка [Електронний ресурс]. – Режим доступу: http:// www.niss.gov.ua/articles/454.

7. Прибуток світової кіберзлочинності за 5 років склав 1 трлн доларів [Електрон. ресурс]. – Режим доступу http://tsn.ua/groshi/pributok-svitovoyi-kiberzlochinnosti-za-p-yat-rokiv-sklav-1-mlrd-dolariv.html.

8. Про внесення зміни до ЗУ "Про ратифікацію Конвенції про кіберзлочинність" (ВВР), 2011, N 5, ст.32) [Електрон. ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/ show/2532-17.

9. Рука Путина: Госдума ввела цензуру в Интернете. [Електрон. ресурс]. – Режим доступу: http://news.liga.net/foreign/world/696772-ruka_putina_ gosduma_vvela_tsenzuru_v_internete_la_republica.htm.

10. С. Брин: Открытость и всеобщая доступность Интернета – основополагающие принципы всемирной сети. [Електрон. ресурс]. – Режим доступу: http://echo.msk.ru/blog/echomsk/879239-echo/

11. SCADA OS: первая в мире защищённая операционная система [Електрон. ресурс]. – Режим доступу: http://www.xakep.ru/post/59488/

12. ООН опубликовала данные о доступности интернета и мобильной связи в мире. [Електрон. ресурс]. – Режим доступу: http://blogs.computerra.ru/42046.

13. По доступности домашнего интернета Украина уступает даже Беларуси. [Електрон. ресурс]. – Режим доступу: http://proit.com.ua/news/ telecom/ 2013/01/17/120040.html.

Надійшла до редколегії 19.03.2013

Рецензент: канд. техн. наук, доцент В.І. Брітик, Харківський національний університет радіоелектроніки, Харків.

К ОПРЕДЕЛЕНИЮ НАПРАВЛЕНИЙ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

В.М. Струков

Статья посвящена анализу причин распространения киберпреступности в Украине и выработке концептуальных путей профилактики и противодействия этому негативному социальному явлению. Исследованы и проанализированы корни таких причин как неурегулированность доступа к киберпространству и услугам в нем, технико-технологические особенности организации киберпространства и несовершенство законодательной базы. В результате проведенного исследования сформулированы концептуальные пути противодействия киберпреступности.

Ключевые слова: *Информационная безопасность, Интернет, операционная система, коммуникационное оборудование, витруальные отношения, сайт, киберпреступление, профилактика.*

TO THE DEFINITION OF THE DIRECTIONS OF COUNTERACTION TO CYBER CRIME

V.M. Strukov

The article is devoted to the analysis of reasons for the proliferation of cybercrime in Ukraine and elaboration of conceptual ways of preventing and counteracting this negative social phenomenon. Researched and analyzed the roots of such reasons as lack of proper access to cyberspace and services in it, technical and technological peculiarities of cyberspace and the imperfection of the legislative base. As result, conceptual directions of countering cybercrime have determined .

Keywords: *Information security, Internet, operating system, communication equipment, virtual relations, site, cybercrime, prevention.*