УДК 343.98

О. В. Орлов,
д.держ.упр., доц.,
завідувач кафедри інформаційних технологій
і систем управління ХарРІ НАДУ,
м. Харків

ДЕРЖАВНЕ УПРАВЛІННЯ ПІДГОТОВКОЮ ФАХІВЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ

Показана необхідність підвищення уваги держави до підготовки фахівців у галузі боротьби з кіберзлочинністю. Проаналізовані методи боротьби зі зловживаннями в комп'ютерних мережах. Надані пропозиції щодо підготовки фахівців по боротьбі з кіберзлочинністю.

Ключові слова: кіберзлочин, кібербезпека, комп'ютерна мережа, загроза, Інтернет, інформаційні технології.

Кібернетична злочинність є не лише технічну і правову, але і соціальну проблему, ефективне рішення якої вимагає, передусім, системного підходу по розробці основ забезпечення безпеки життєво важливих інтересів громадянина, суспільства і держави в кіберпросторі.

У загальному розумінні під системою протидії кібернетичної злочинності прийнято розуміти взаємопогоджену діяльність органів виконавчої влади, організацій і підприємств усіх форм власності (передусім, громадських організацій і IT-бізнесу) за такими напрямками:

– дослідження і оцінки кібернетичних загроз, форм і методів її організації, а також рівня кібернетичної безпеки в реальних умовах інформатизації суспільства і держави;

– вдосконалення законодавства з питань кібернетичної безпеки відповідно до міжнародних норм на рівні ООН, Інтерполу, НАТО, Європейського Союзу та ін.;

– здійснення ефективних заходів попередження, протидії й розслідування кібернетичних злочинів;

– підготовка фахівців кібернетичної безпеки.

Проблематика підготовки національних кадрів у сфері інформаційних технологій та кіберебезпеки досить часто обговорюється фахівцями в інформаційній сфері в наукових журналах, на наукових конференціях, семінарах, круглих столах і в засобах масової інформації. Деякі аспекти підготовки кадрів в сфері інформаційних технологій вивчали К. Бєляков, В. Бутузов, В. Голубєв, Н. Дубова, С. Кльоцкін, В. Кудінов М. Литвинов, В. Мохор, Е. Рижков, В. Хахановський, І. Хараберюш та ін.

Проблематика підготовки кадрів в інформаційній сфері, міжнародний досвід організації навчального процесу, досягнення й пропозиції у сфері боротьбі з кіберзлочинністю обговорюється в статтях В. Бачило, О. Бєлоусова, В. Голубєва, К. Гур'янова, Н. Дубової, В. Козлова, Г. Маклакова, В. Поліванюка, О. Нєхорошева, Є. Тітуніної. Проте наразі недостатньо ґрунтовних досліджень з проблем підготовки фахівців з протидії злочинам у сфері кібербезпеки.

Мета статті – дослідити та проаналізувати проблеми, які виникають при підготовці кадрів правоохоронців з протидії злочинам в галузі інформаційних технологій та кіберзлочинності і надати пропозиції щодо створення єдиної загальнодержавної системи протидії кібернетичної небезпеки й підготовки кадрів для такої системи.

Сьогодні у світі дослідженню проблем боротьби з кіберзлочинністю приділяється значна увага, що обумовлено об'єктивними процесами розвитку інформаційно-телекомунікаційних технологій і їх впровадженням в різні сфери громадської діяльності.

Кіберзлочинність стала одним із п'яти найпоширеніших економічних злочинів в Україні. Кожен третій респондент (37 %) вважає, що ризик кіберзлочинності підвищився за останні 12 місяців. Понад 25 % організацій не мають відповідних політик та механізмів реагування на кіберзлочини. 46 % опитаних не проходили навчання у сфері кібербезпеки впродовж останніх 12 місяців. 58 % респондентів з України заявили, що в їхніх організаціях відсутній процес моніторингу відвідування соціальних мереж [1].

До останнього часу кіберзлочинність у нас асоціювалася переважно з різними видами махінацій з банківськими картами клієнтів-фізичних осіб. Так, злочинці з допомогою спеціальних пристроїв (наприклад, так званих скімерів, які встановлюються на банкоматах) одержували дані клієнтів і виготовляли дублікати карт для подальшого зняття грошей з рахунків. За оцінками НБУ, торік питома вага подібних шахрайств становила 0,002 % від загального обсягу операцій з картками. Із цим явищем банки і правоохоронці, як вони запевняють, загалом уже навчилися боротися. Про це свідчить у тому числі збільшення кількості виявлених скімерів (2013 р. – близько 160, 2012 р. – 73, 2011 р. – 45).

За словами начальника управління по боротьбі з кіберзлочинністю МВС України М. Литвинова, 2013 р. вже зафіксовано понад 270 спроб несанкціонованого списання коштів з рахунків клієнтів банків на загальну суму більш як 108 млн грн [2].

За даними Управління боротьби з кіберзлочинністю МВС України, найбільш поширеними видами кіберзлочинів є: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів) та несанкціоновані дії з інформацією, яка ними оброблюється. За 10 місяців 2012 р. зафіксовано 44 таких втручання.

За даними Державної служби фінансового моніторингу України, у 2012 р. було зареєстровано 179 спроб несанкціонованого доступу до рахунків клієнтів банків на загальну суму понад 150 млн грн, при цьому сума коштів, у подальшому знятих злочинним шляхом лише готівкою, становить 9,5 млн грн. [3].

З урахуванням створення загальнодержавної системи кібернетичної безпеки шляхом координації діяльності виконавчої влади із залученням ініціативи приватного сектора і громадських організацій, важливо уникнути зіткнення термінів. Чітке і однозначне тлумачення основних понять дозволить визначитися і з відомчими сферами компетенції, і особливостями підготовки фахівців розслідування і розкриття кіберзлочинів.

Кіберзлочин - громадське небезпечне діяння, за яке встановлюється карна

відповідальність (кібератаки, інші традиційні злочини, здійснювані за допомогою сервісних можливостей і інформаційних ресурсів інформаційно-телекомунікаційних систем – ІТС). На сьогодні в мережі відомі декілька класифікацій кіберзлочинів.

Згідно з класифікацією, запропонованою X Конгресом ООН, кіберзлочини можна розділити на ті, які здійснюються проти ІТС (кіберзлочини у вузькому розумінні) і за допомогою ІТС (кіберзлочини в широкому розумінні) [4].

Конвенція про кіберзлочинність ділить її на наступні категорії:

– правопорушення проти конфіденційності, цілісності і доступності комп'ютерних систем;

– правопорушення, пов'язані з комп'ютерами;

– правопорушення, пов'язані з дитячою порнографією;

– правопорушення, пов'язані з порушенням авторських прав [5].

Таким чином, технічна складова усіх можливих видів злочинів є однаковою і не залежить від того, чи йде мова про злочини проти конституційних прав особи, майнових прав людини або злочинів в економічній сфері або проти громадської і державної безпеки.

Уявляється, що технічна складова підготовки фахівців з кібернетичної безпеки також є однаковою і незалежною від відомчих сфер компетенції в питаннях забезпечення кібернетичного захисту особи, суспільства і держави.

Таким чином, з урахуванням широкого використання можливостей кіберпростору для здійснення вже відомих і передбачених кримінальним кодексом злочинів, виникає необхідність вдосконалення системи протидії кіберзлочинності, розмежування компетенцій правоохоронних і інших державних органів в питаннях вказаної протидії на порядок денний знову виноситься теза про створення системи підготовки, перепідготовки і підвищення кваліфікації співробітників відповідних держструктур.

Про важливість інформаційного і кіберпростору нині свідчить поява концепцій ведення в них і створення у збройних силах декількох держав

спеціалізованих структур, призначених для здійснення так званого інформаційного протиборства.

Співробітники згаданих спеціалізованих структур до визначення (терміну) кібербезпеки відносять своєчасне виявлення, попередження, нейтралізацію реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і (чи) національним інтересам, що натомість фактично:

1. Дає можливість говорити про формування принципово нової геостратегічної, геоінформаційної і геополітичної ситуації, коли виникають зовсім нові загрози безпеки для об'єктів критично важливої інфраструктури цих держав, їх окремих громадян і суспільства в цілому, і, безумовно, виводить на найвищий ієрархічний рівень значущість досліджень, спрямованих на усебічний аналіз методів, засобів, тактики і стратегії дій в інформаційному і кіберпросторі.

2. Обумовлює необхідність вироблення рекомендацій відносно короткострокових і довгострокових пріоритетів трансформації сектора безпеки цих держав за напрямами:

– проведення кардинальних змін засобів і способів обміну інформацією;

– створення спеціальних програмно-апаратних комплексів розвідки в інформаційному і кібернетичному просторах для вирішення завдань по пошуку і добуванню відомостей, даних і знань;

– створення комплексних систем захисту власних інформаційного і кіберпростору, інформаційно-комунікаційних технологій (ІКТ) і ІТ-систем від внутрішніх кібернетичних втручань (спроб впливу протиборчих сторін на інформаційне і кіберпростору один одного за рахунок використання засобів сучасної обчислювальної і (чи) спеціальної техніки, і відповідного програмного забезпечення) і кібернетичних загроз (проявів дестабілізуючого негативного впливу протиборчих сторін на певний об'єкт, що реалізується за рахунок використання техніко-логічних можливостей інформаційного і кібернетичного просторів, створюючи при цьому небезпеку як для них самих, так і свідомість

людини в цілому).

З урахуванням викладеного вище, можна стверджувати, що характерною ознакою, що обумовлює поняття кібербезпека, являється сукупність активних захисних і розвідувальних дій, які в процесі інформаційного протиборства зусиллями інсайдерів-одинаків або організованих кіберугруповань розгортаються навколо ІР, і які спрямовані на досягнення і підтримку потенційними супротивниками переваги в протидії новим загрозам безпеки для об'єктів їх критично важливої інфраструктури.

Підготовка фахівців в галузі боротьби з кіберзлочинністю. Спробуємо виділити найбільш важливі аспекти в дослідженні з урахуванням сучасного розвитку ІТ-технологій і зміст освіти фахівців, які повинні працювати у сфері попередження кіберзлочинів.

Передусім, у фундамент комп'ютерних інцидентів необхідно закласти нормативно-правове і доктринальне значення таких термінів, як «комп'ютерний інцидент» і «інцидент» взагалі. Відобразити їх співвідношення. Показати місце в класифікації саме комп'ютерних інцидентів в технічному і юридичному сенсах, представити ієрархію інцидентів як явища.

Розгляд цього аспекту з позиції об'єднання юридичної і технічної науки дозволить нам, шанований читач, найефективніше здійснювати дослідження комп'ютерних інцидентів з метою їх попередження, локалізації, блокування і профілактики.

Наступним важливим моментом з точки зору відробітку системного підходу є розробка технічної складової процедури дослідження комп'ютерних інцидентів.

Важливим є не лише і не стільки фіксація фактів порушень встановлених норм політики безпеки, скільки їх класифікація.

У цьому випадку критерієм може служити співвідношення прогнозованих збитків і грошових коштів, необхідних для відновлення працездатності системи і протидії подібним втручанням в майбутньому.

З урахуванням викладеного підходу до порушень політики безпеки,

українського і міжнародного досвіду в цій сфері, виділимо в наших діях наступні етапи:

1. Реагування на комп'ютерні інциденти:

– комп'ютерно-технічна або криміналістична експертиза. Що включає відновлення хронології події, аналіз журналу файлової і операційної систем, вивчення ключів реєстру операційної системи, дослідження носіїв на наявність шкідливого програмного забезпечення, повний аналіз шкідливого програмного забезпечення, відновлення видаленої інформації, пошук і вивчення інформації на носії відповідно до поставленого завдання, оформлення звіту;

– збирання доказової бази;

– виявлення причин виникнення інциденту;

– розробка і видача рекомендацій мінімізації ризиків;

– юридичне оформлення всієї звітності;

– висновки про можливість, доцільність юридичного переслідування.

2. Розслідування комп'ютерних інцидентів:

– проведення роботи з виявлення (добування) інформації, що дозволяє ідентифікувати правопорушника;

– збирання і оформлення матеріалів для ухвалення рішення про їх передачу правоохоронним органам;

– супровід і підтримка на етапі здійснення процесуальних дій;

– супровід і підтримка вже на етапі судового розгляду;

– загальний юридичний супровід матеріалів справ по розгляду комп'ютерних інцидентів.

З урахуванням багатоаспектності цієї проблематики, її виходу за межі буденного, вірніше вузькоспрямованого сприйняття комп'ютерних інцидентів як ІТ-спеціалістами, так і правоохоронцями, особливе значення придбаває зміст підготовки відповідного персоналу.

Тут головною метою освіти повинне стати формування розуміння неприпустимості комп'ютерних інцидентів і високої громадської небезпеки їх наслідків. Передусім, потрібна базова освіта в області ІТ-технологій. Але воно

не повинне дублювати спеціалізовані курси системних адміністраторів і програмістів. Найважливішими складовими є формування поняття кіберзлочинів, розрізнення злочину і провини, видів відповідальності.

Доцільно прислухатися до думок ІТ-спеціалістів при розробці відповідних нормативно-правових актів. Також корисними виявляться знання у сфері досліджень, розслідувань і розгляду в судових інстанціях відповідних матеріалів, по яких притягувалися фахівці як експерти і консультанти.

Адже проблеми дослідження комп'ютерних інцидентів можна вирішити і вирішувати надалі тільки при тісній взаємодії усіх зацікавлених представників держави і суспільства.

Принципово нові можливості, які сьогодні виникають завдяки завоюванню переваги в інформаційно-психологічній сфері, мають в розпорядженні низку особливостей:

– скритність і анонімність операції інформаційно-психологічними впливами, можливість проведення їх «під чужим прапором» і з будь-якої точки інформаційного простору, кіберпростору;

– «плавність» перемикання інформаційних впливів, регульована в широких рамках інтенсивність і тривалість їх реалізації : від організації інформаційних «шоків», «ударів», «блокад» до уповільнених, латентних, розтягнутих на роки мікродозованих впливів;

– багатоаспектність впливу з високою мірою координації в часі і просторі. Зростання насиченості усіх сфер життя суспільства інформаційними системами і технологіями дає можливість монтувати інформаційні впливи адекватно прийнятому алгоритму впливу на різні сфери, процеси, країни об'єкти, групи, персони одночасно, в необхідній послідовності і під різними «кутами впливу». Це дозволяє оптимізувати отримання необхідного кінцевого результату і витрати на його досягнення;

– здатність малими інформаційними впливами досягати значних кінцевих результатів;

– перенесення функцій озброєного стримування на інформаційну сферу.

Провідні держави світу орієнтуються на превентивні заходи в реалізації функцій стримування;

– створення хаосу в обраній для інформаційного впливу державі і подальше управління ним (чи з його допомогою) як один із шляхів досягнення необхідних результатів.

Забезпечення інформаційної безпеки, як і будь-який процес забезпечення, може досягти мети за умови дотримання трьох умов :

– визначення і опис конкретних завдань для системи (характеристика завдань, їх можливий обсяг і т. ін.) і наявність суб'єктів, здатних вирішувати ці завдання;

– наявність суб'єктів системи, які б здійснювали організацію процесу забезпечення і управління таким процесом;

– наявність сил і засобів безпосереднього здійснення захисту життєво важливих інтересів держави в інформаційній сфері.

Немає державного суб'єкта у сфері інформаційної безпеки, наділеного необхідними повноваженнями і забезпеченого відповідним науковим і кадровим потенціалом. В зв'язку з цим забезпечення інформаційної безпеки країни обумовлює детальніше обґрунтування потреби в організації ефективної протидії спеціальним інформаційним операціям, що масово проводяться проти України. Особливо, що стосується нейтралізації деструктивних інформаційно-психологічних впливів з боку інших держав, захисту життєво важливих інтересів громадянина і суспільства в інформаційній сфері.

Останніми роками в мережі все частіше з'являються сайти, основною функцією яких є негласний доступ особистої інформації їх відвідувачів: номери платіжно-розрахункових карт і PIN-коди до них; логіни і паролі; адресна книга; історія відвідувань і закладки у браузері; нещодавно збережені документи та ін.

Принципи дій таких сайтів різні. Скажімо, користувач, працюючи в Інтернеті, при переході по посиланню або допускаючи клік «правою мишкою» по рекламному банеру потрапляє на сторінку, де спеціальна програма, користуючись уразливістю в захисті операційної системи і (чи) браузеру,

запускає завантаження програми-вірусу («троянського коня») на комп'ютер жертви, який заражає систему. Такий «комп'ютер-зомбі» може віддалено контролюватися хазяїном вірусу.

В інших і, скажімо так, найбільш поширених випадках, жертва вводить на порталі свої персональні дані, сприймаючи його як надійний інтернетівський ресурс з високою мірою довіри.

Як відомо, такі шахрайські сайти-пастки називаються фішинговими (від англ. fishing – рибальство). Злочинці освоюють метод соціальної інженерії з метою отримання конфіденційних даних від довірливих і недосвідчених користувачів. Такі псевдодовірені сайти є однією з форм злочинного застосування цього методу.

Соціальна інженерія – метод управління діями особи, заснована на використанні слабостей людського чинника. Найбільш частіше соціальну інженерію розглядають як незаконний метод отримання інформації, проте такий погляд не зовсім правильний. Соціальну інженерію можна і треба використовувати із законними цілями, наприклад, для отримання оперативної інформації від самого зловмисника.

Сайти-пастки дають можливість досягти різних цілей в профілактиці і боротьбі з кіберзлочинністю. Залежно від цілей обираються методи дій оперативних працівників.

Розглянемо коротко деякі цілі і методи їх досягнення :

1. Встановлення IP-адреси користувача і подальше встановлення його особи.

Суттю цього методу є створення сайту будь-якої тематики і виду з розміщенням на нім програмного коду лічильника відвідувачів, з можливістю фіксації IP-адресу і часу відвідування кожним мирянином кіберпростору.

Нижче наводяться дані, що фіксуються стандартним лічильником: IP-адреса комп'ютера користувача; точний час і дата відвідування сайту; деякі відомості про провайдера інтернетівських послуг користувача; географічне положення комп'ютера користувача; тип підключення до Інтернету; версія

браузеру (програми для перегляду інтернет-сторінок); версія операційної системи; установки розподільної здатності монітора.

Таким чином, вищевикладену інформацію лічильника відвідувань можливо використовувати з метою з'ясування інформації за IP-адресою зловмисника за умови, що він був відвідувачем сторіночки, на якій заздалегідь був встановлений такий лічильник.

Для реалізації вищезгаданого методу оперативному працівникові необхідно виконати наступні дії:

– створити шаблон веб-сторінки, встановивши на нього код лічильника і розмістити цей шаблон в Інтернеті;

– направити зловмисникові послання (лист, посилання під час чату і ін.) на цю сторіночку з пропозицією її перегляду;

– перевірити статистику відвідувань створеної сторіночки з лічильником на сайті з метою встановлення інформації про його IP-адресу;

– встановити провайдера інтернет-послуг, до мережі якого належить IP-адреса;

– встановити місцезнаходження комп'ютера, що входив в кіберпростір в указаний час під встановленою IP-адресою.

Такий метод виявиться дієвим при встановленні особи, автора анонімних повідомлень злочинного характеру на інтернет-ресурсах, наприклад, оголошень про надання послуг або товарів, заборонених законом.

2. Залучення представників протиправних професій на спеціально створений для спілкування тематичний ресурс з метою контролю їх спілкування і отримання оперативної інформації.

Цей метод на практиці реалізується мінімум двома шляхами:

– створенням і розвитком інтернет-ресурсу для контролю активності його учасників;

– впровадженням (вербуванням) одного з активних учасників з правами адміністратора порталу.

3. Дослідження актуальних методик хакерських атак.

Цей метод більше торкається фахівців безпеки інтернет-ресурсів і захисту інформації, оскільки в переважній кількості випадків носить дослідницький характер.

Суть методу полягає в створенні локальної мережі-приманки, тобто одного з різновидів пастки. Наживкою виступає захищений ресурс, призначення якого полягає в тому, щоб виступати об'єктом зондування атак і зломів з боку хакерів. З цією метою створюється сайт, на якому не ведеться ніяка змістовна діяльність (він не використовується). Це означає, що якщо кимось в таку пастку передається пакет даних або хтось робить спробу отримати доступ до ресурсу, то, найшвидше, подібні дії є зондуванням, скануванням або атакою.

Попри те, що сфера застосування таких пасток досить обмежена (вони здатні відстежувати лише ті атаки, які спрямовані безпосередньо проти пастки), з їх допомогою можна домагатися ефективнішого використання вже наявної архітектури захисту.

Основне призначення таких ресурсів – стати об'єктом атак хакерів. Після кожного зареєстрованого факту атаки зібрана інформація ретельно аналізується. До речі, будь-який охочий має реальну можливість приєднатися до цього проекту і результатів досліджень через сайт організації.

Таким чином, в розріз сформульованої громадської думки про фішинг і соціальну інженерію як методи злочинної діяльності, вони, ці методи, можуть і мають бути використані в профілактиці і боротьбі із злочинністю в Інтернеті.

Незважаючи на цілком зрозумілу інертність правоохоронної свідомості, використання ними нині нових і оновлених, оперативно-розшукових сил, засобів і методів об'єктивно значно актуалізується, передусім, у зв'язку з появою такого феномену, як кіберзлочинність.

В останні роки технічний прогрес, що супроводжується масовою комп'ютеризацією усіх сторін життя суспільства, об'єктивно детермінував криміналізацію сфери використання комп'ютерної інформації, що, у свою чергу, викликало необхідність встановлення відповідальності перед законом за

скоєння таких злочинів.

Хотілося б, щоб реалізація на практиці викладених побажань сприяла підвищенню ефективності протидії поліції і спецслужб злочинам, що здійснюються у сфері комп'ютерної інформації.

Особи, що займаються розслідуванням цього роду злочинів, і працівники судової системи у більшості своїй не мають спеціальних знань у сфері нових комп'ютерних технологій, що спричиняє помилки в кваліфікації та розслідуванні злочинів. Також причинами помилок є відсутність достатньої кількості рекомендацій і роз'яснень по розслідуванню злочинів у сфері інформаційних технологій, відсутність узагальненої судової практики по кіберзлочинності і відсутність в правоохоронних органах необхідного числа фахівців, що розбираються в сучасній техніці і здатних оперативно виявляти і розслідувати комп'ютерні злочини. У зв'язку з цим виникає завдання введення нових спеціалізацій і внесення змін до учбового плану підготовки студентів юридичних ВНЗ, курсантів і слухачів спеціальних навчальних закладів.

Список використаних джерел:

1. Україна. Всесвітній огляд економічних злочинів – PwC [Електрон. ресурс]. – Режим доступу : https://www.pwc.com/ua/uk/.../GECS_Ukraine_ua.pdf.

2. Кіберзлочинність: прихована і явна загроза [Електрон. ресурс]. – Режим доступу : http://gazeta.dt.ua/macrolevel/kiberzlochinnist-prihovana-i-yavna-zagroza-_.html.

3. Заступник міністра внутрішніх справ України Сергій Лекарь взяв участь у всеукраїнській науково-практичній конференції «протидія кіберзлочинності у фінансово-банківській сфері» [Електрон. ресурс]. – Режим доступу : http://mvs.gov.ua/mvs/control/pz/uk/publish/article/83452;jsessionid=8F2ABCD7D35CFC3E45944D4EAC556581.

4. Киберпреступность. Что это? [Електрон. ресурс]. – Режим доступу : http://elcomrevue.ru/kibeoprestupnost-chto-eto/

5. Конвенція про кіберзлочинність / Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 р. [Електрон. ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_575.

6. Правове регулювання інтернету в Росії [Електрон. ресурс]. – Режим доступу : http://finance-dom.ru/marketing/81/412-pravove-regulyuvannya-internetu-u-rosi%D1%97.

Orlov O. V. **Public administration of training cyber security experts.**

The necessity for focusing government attention on training in cybercrime control is proved. The methods of combating abuses in computer networks have been analyzed. Suggestions for training experts in cybercrime countermeasures are provided.

Key words: cybercrime, cyber security, computer network, threat, Internet, information technologies

Орлов А. В. **Государственное управление подготовкой специалистов в области кибербезопасности**

Показана необходимость повышения внимания государства к подготовке специалистов в области борьбы с киберпреступностью. Проанализированы методы борьбы со злоупотреблениями в компьютерных сетях. Представлены предложения по подготовке специалистов по борьбе с киберпреступностью.

Ключевые слова: киберпреступности, кибербезопасность, компьютерная сеть, угроза, Интернет, информационные технологии