УДК 025.22:004.7:004.056.53

Світлана Горова,
канд. наук із соц. комунікацій, ст. наук. співроб. ФПУ Національної бібліотеки України імені В. І. Вернадського

СПЕЦИФІКА БІБЛІОТЕЧНОГО КОМПЛЕКТУВАННЯ В УМОВАХ АКТИВІЗАЦІЇ ІНФОРМАЦІЙНОЇ ЗЛОЧИННОСТІ

Розглянуто основні проблеми, пов'язані з актуалізацією теми кіберзлочинності у зв'язку з активним розвитком інформаційних і телекомунікаційних технологій, доступом до виробництва та використання інформаційних ресурсів усіх категорій населення, у тому числі й тих, що схильні до правопорушень, у контексті чого з'явилося таке явище як хакерство, кібертероризм, що вносить в інформаційні процеси протиправні елементи, негативно впливаючи на розвиток національного інформаційного простору України.

Ключові слова: кіберзлочинність, хакери, комплектування, інформаційний простір, шкідлива інформація, бібліотечні фонди.

Постановка проблеми. Розглядаються основні загрози, що виникають унаслідок діяльності кіберзлочинців й негативно впливають на вітчизняну інфосферу.

Розробкою питань інформаційної безпеки та кіберзлочинності займаються вітчизняні та зарубіжні науковці, а саме М. Кастельс, М. Моїсєєв, Е. Тоффлер, В. Горовий, В. Бутузов, В. Петрик, М. Присяжнюк та ін., проте сучасний стрімкий розвиток інформаційного суспільства постійно дає новий матеріал для науково-практичних узагальнень.

Актуальність дослідження обумовлена зростанням суспільної важливості національної інформаційної безпеки в умовах загострення сучасних інформаційних протистоянь.

Метою статті є розгляд характерних проявів кіберзлочинності в умовах сучасної інформатизації, визначення її основних загроз для інформаційного розвитку суспільства, для комплектування суспільно значущими інформаційними ресурсами фондів бібліотек.

Розвиток нових інформаційних і комунікаційних технологій у наш час забезпечив доступ до інформаційних ресурсів усіх категорій громадян України, розкрив нові можливості та став стимулом для зростання соціальної активності членів суспільства, для розвитку всіх сфер

суспільного життя, його соціокомунікаційних властивостей та структур. Цей процес, сприяючи розкриттю творчих можливостей людей, забезпечує зростаючу життєздатність самих соціальних структур і необхідну адекватність реагування сучасного суспільства на весь комплекс викликів, що ставить перед ним сьогодення.

Однак, окрім беззаперечно корисного та необхідного для суспільства змісту, активізація інформаційно-комунікаційних процесів може нести в собі й певні загрози, зокрема з боку кіберзлочинності. Таким чином, актуалізується проблема дослідження та об'єктивної оцінки можливих загроз з боку продукованих кіберзлочинцями ресурсів, зокрема й тих, що пов'язані з можливим поширенням через бібліотечну мережу при неуважному комплектуванні новою електронною інформацією, у яку потрапляють шкідливі, провокативні закладки.

До цього ж необхідно звернути увагу також на ту обставину, що у зв'язку з подіями на Сході України, концентрацією суспільної уваги, уваги правоохоронних органів до АТО, зростання кіберзлочинності в Україні в недалекому майбутньому може мати додатковій поштовх без відповідного посилення реакції з боку правоохоронних органів. Зростаюча кіберзлочинність, таким чином, може стати істотною перешкодою на шляху трансформації українського суспільства, підвищення його економічної, а також і політичної ефективності.

Необхідно зазначити, що серед кіберзлочинців найбільш помітним з початком розвитку електронних технологій у нашій країні стало хакерське, віртуальне співтовариство. Характеризуючи розвиток цього специфічного для інформаційного суспільства співтовариства, М. Кастельс не лише зауважує те, що його члени одержують задоволення від здобуття певного статусу у співтоваристві, від радості творчості, від зближення зі світом мистецтва, психологічним збудженням – «драйвом» від процесу творіння, він говорить про розвиток характерного для цієї категорії людей «почуття вищості над усім іншим комп'ютерно безграмотним світом і тенденції спілкування з комп'ютером або з іншими представниками людства за посередництва комп'ютерів, зосереджуючись винятково на питаннях програмного забезпечення, незрозумілих для решти людства» [1]. Дослідник звертає увагу також на те, що, на думку лідерів хакерського руху, лише тоді, «коли люди задовольнили свої базові потреби, вони можуть дозволити собі присвятити життя інтелектуальній творчості й лише потім діяти в умовах культури дарування» [2].

Учені звертають увагу також на те, що якісно вищий, порівняно з традиційним, рівень спілкування в ІТ-субкультурі дав змогу швидко

сформувати систему внутрішньокультурних ціннісних критеріїв, певні етичні норми, критерії успішності, задоволення естетичних і пізнавальних потреб, критично безмежних комунікативних можливостей, розвитку інтернет-бізнесу і навіть своєрідного інтернет-спорту у вигляді хакерства [3].

Враховуючи той факт, що хакери у своїх захопленнях завжди опираються на найновіші здобутки комп'ютерної науки, техніки та технологій, і що за цими здобутками зазвичай не встигає і міжнародна правова база, і правотворення на рівні окремих держав, об'єктивно хакерські маніпуляції в основному своєму змісті перебувають за межами регулювання закону. Щоправда, у засобах масової інформації час від часу з'являються повідомлення про використання здібностей талановитих хакерів в інтересах реалізації певних завдань інформаційних воєн – нової форми взаємовідносин інформаційного суспільства, – про створення відповідних секретних підрозділів в оборонних відомствах, насамперед, провідних країн-глобалізаторів. Однак, за тими ж повідомленнями, до роботи в цьому напрямі залучаються, як правило хакери, що вже були помічені в протиправних діях: на зламах електронного захисту та грабуванні банків, у несанкціонованому входженні в комп'ютерні системи управлінських структур, у протиправних заходах економічної розвідки та ін.

Характерна для сучасного рівня розвитку інформаційного суспільства та рівня правового забезпечення діяльності у сфері застосування електронних інформаційних технологій в Україні ситуація, у цілому ж, не сприяє використанню хакерського руху в інтересах суспільного розвитку. Тобто наше суспільство, як і в більшості країн світу, не знаходить поки що способу використання творчого потенціалу найбільш освічених і компетентних своїх членів, таких, що найкраще знаються на електронних інформаційних технологіях, які є локомотивом розвитку інформаційного суспільства.

Проте нові можливості, що з'явилися в результаті розвитку інформаційних технологій, стали широко використовуватись представниками кримінального світу. А це, у свою чергу, призвело і до появи нових видів злочинів, пов'язаних, зокрема, з незаконним втручанням у роботу систем і комп'ютерних мереж, розкраданням і несанкціонованою зміною та поширенням даних або інформації та ін. Відповідно, кіберзлочинність перетворилася на чинник, який став здійснювати вагомий тиск на суспільні відносини. Дослідники зазначають, що сьогодні кіберзлочинність стала «багатоголовою гідрою», зважаючи на такі її характеристики як транснаціональність, латентність, динамічність темпів зростання та трансфор-

мацій, анонімність, масштабність наслідків, тощо. В умовах глибокого латентного проникнення кіберзлочинності в суспільне та державне життя, її подолання стає наріжним каменем на шляху розбудови інформаційного суспільства та входження України у світовий інформаційний простір [4].

При цьому необхідно звернути увагу ще й на таку нині існуючу тенденцію: наша країна з її низьким рівнем обізнаності про загрози використання комп'ютерів і низьким рівнем інформаційної безпеки стає для програмістів-хакерів справжнім клондайком. Шахрайство в інформаційних мережах, інсайдерські витоки інформації, поширення шкідливої, неправдивої інформації стають повсякденними явищами.

При цьому привертає до себе увагу одна з найпоширеніших схем, впроваджених в інформаційний простір кіберзлочинцями: викладення в електронних ЗМІ за допомогою злому сайтів неправдивих новин чи будь-якої іншої шкідливої інформації [5].

Про існуючі небезпеки від кіберзлочинів, що за способом вчинення належать до інформаційної групи, зауважує А. Бабенко. Він вказує, що такі злочини здійснюються шляхом використання незаконних способів отримання інформації, зокрема, через несанкціонований доступ до комп'ютерів і мереж, а також поширення неправдивої інформації [6].

При цьому необхідно зазначити, що будь-яка інформація, кваліфіковано введена до цільової спільноти, одразу тиражується та поширюється без перевірки. Одним з недавніх показових прикладів можна назвати повідомлення Чернігівської обласної державної телерадіокомпанії про те, що «хакери атакують патріотичні українські групи і пишуть там неправдиву інформацію. Сіють паніку і серед родин, чиї чоловіки перебувають у зоні АТО, особливо коли батальйони вступають в активну фазу боїв. Від імені офіційних українських джерел російські хакери виходять і на ЗМІ та розповсюджують інформацію, яка не відповідає дійсності» [7].

ЗМІ інформували також про неодноразові зломи сайту прес-центру антитерористичної операції. Сайт атакувався хакерами, у результаті чого на ньому була подана недостовірна інформація [8].

Відповідно, необхідно зазначити, що при фіксації в інформаційних базах оперативних матеріалів, що відображають важливі суспільно значущі події, необхідним є уважне вивчення всього контексту матеріалів і визначення на цій базі їх достовірності.

Доволі частими на сьогодні є атаки хакерів і у соціальних мережах. Так, нещодавно в соціальній мережі Facebook, згідно з інформацією

прес-аташе народного депутата С. Семенченка, інформаційна сторінка батальйону «Донбас» була зламана хакерами, які розмістили на ній неправдиву інформацію [9].

Керівник програм нових медіа в Internews-Україна В. Мороз у своєму коментарі стосовно «роботи» хакерів у соціальних мережах зазначив: «Сепаратисти створили фейковий прес-центр АТО. Вони використали ідентичність цієї сторінки, вони викрали аватар, фото, опис повністю. І вони почали публікувати зміст з позиції терористів. Звісно, була велика кількість скарг, і через деякий час фейковий прес-центр АТО був заблокований» [10]. Проте інформація вже поширилась в інтернет-просторі…

У ЗМІ також вказували й на неодноразові хакерські атаки з боку «КіберБеркуту». Блокуванню піддавався сайт Президента України. Члени організації звинуватили П. Порошенка в геноциді власного народу й зануренні країни в убогість і хаос. Раніше ця ж організація блокувала сайти МВС та Генпрокуратури. Хакери вимагали звільнити бійців «Беркута», затриманих за звинуваченням у розстрілі євромайданівців [11].

Зростаючий рівень кіберзлочинності в Україні показують дані XVI випуску звіту Microsoft Security Intelligence Report (SIRv16), у якому проаналізовано вразливість і загрози негативних впливів на більше мільярда систем і популярних сервісів по всьому світу. Україна очолила антирейтинг країн, у яких налічується найбільша кількість сайтів, що містять шкідливі програми. Дослідження виявило, що кожен 16-й сайт в Україні містить шкідливе програмне забезпечення, яким потенційно може бути заражений комп'ютер користувача. Так, на 1000 хостів припадає 59,2 заражених сайтів. Це найвищий показник у світі (для порівняння, у всій мережі Інтернет в середньому заражений приблизно кожен 54-й ресурс).

З усіх проаналізованих у звіті країн в Україні також виявлено найвищу концентрацію фішингових сайтів – кожен 70-й ресурс є шахрайським. Згідно з дослідженням, більш ніж кожен двохсотий сайт в Україні містить експлойти, які аналізують уразливості в системі і можуть ініціювати завантаження небажаних файлів на комп'ютер користувача без його відома [12].

Експерти у своїх коментарях також зазначають, що Україна – помітний центр хакерства, поряд з Росією, Бразилією, Китаєм і меншою мірою – Індією. У цих країнах доволі освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування. Однак в експертних колах існує й інша думка про те, що кіберзлочинність

не є негайною загрозою для українців. Адже наша країна має один із найнижчих у Європі рівнів підключення до Інтернету.

Проте, незважаючи, а, можливо, всупереч вищенаведеному експертному твердженню, необхідно звернути увагу на дані німецького оператора зв'язку Deutsche Telekom, наведені начальником управління інформаційної безпеки Креді Агріколь банку А. Кузьміною, яка вказала, що Україна за рівнем міжнародної кіберзлочинності може випереджати інші країни, адже вона перебуває на четвертому місці у світі після Росії, Тайваню та Німеччини за кількістю кібератак, що виходять із країни. «Щомісяця з українських серверів запускається понад 500 тис. шкідливих програм», – констатувала А. Кузьміна [13].

Сказане вище дає підстави для думки про те, що сучасний науково-технічний прогрес не забезпечує надійного захисту суверенних масивів інформації від шкідливих впливів, від ресурсів, продукованих кіберзлочинцями, навіть за умови високого рівня економічного, техніко-технологічного розвитку, забезпеченого суспільством. Більше того, з розвитком глобального інформаційного простору, процесів інформатизації в усьому світі суверенні масиви інформації ставатимуть дедалі більш вразливими до таких впливів, традиційні уявлення про забезпечення інформаційного суверенітету ставатимуть дедалі менш ефективними в їх практичній реалізації.

Інтереси інформаційної безпеки диктують необхідність постійного моніторингу всіх джерел інформаційного виробництва, своєчасного реагування на можливі інформаційні загрози, пов'язані із введенням у суспільний обіг нової інформації. Неякісна за змістом інформація, шкідлива та небезпечна для суспільства, впливає на громадську думку одразу ж після введення її в систему існуючих у суспільстві соціальних комунікацій. І на цій її властивості ґрунтуються технології розвитку глобальних впливів на національний інформаційний простір у кожному з регіонів світу. На таких інформаційних впливах, поряд з використанням технічних засобів порушення нормальної роботи системи соціальних інформаційних комунікацій противника, базуються стратегії ведення інформаційних війн, як орієнтованих на здобуття самостійного результату, так і як паралізуючого інформаційний простір тієї чи іншої держави.

Поряд із здійсненням оперативного впливу на потенційного противника з допомогою нової інформації сучасні інформаційні технології створюють широкі можливості для довготривалого інформаційного впливу на об'єкт інформаційної атаки шляхом сприяння введенню відповідної інформації в інформаційні бази, зокрема бібліотечні, у систему суверенних

інформаційних ресурсів нації чи держави. Така ситуація є доволі небезпечною, оскільки сприяє довготривалим негативним впливам, руйнуванню національної самобутності, державницьких традицій, веде до однобокої та безперспективної для подальшого розвитку уніфікації.

У зв'язку з цим необхідне проведення організаційних, правових, наукових заходів для активізації участі в роботі з відстоювання національної інформаційної безпеки в умовах посилення глобальних інформаційних впливів наукових установ, аналітичних та інших інформаційних центрів. Особлива увага при цьому має приділятися на сьогодні ще широко розгалуженій в Україні системі бібліотечних та архівних установ, у яких зберігаються основні фонди суспільно значущої інформації і які займаються оновленням цих фондів, відбором для комплектування інформації з її новостворених масивів.

Відповідно, необхідно зазначити, що на сьогодні комплектування фондів бібліотечних установ ресурсами з вітчизняного інформаційного простору потребує підвищення кваліфікації бібліотечних працівників. Зокрема, вони, по-перше, – повинні вміти професійно співставляти та порівнювати офіційні дані та повідомлення з інформацією з інших джерел, які можуть нести відповідні загрози, оперативно знайомитися з технологічними здобутками, що спрямовуються на нейтралізацію цього виду загроз.

По-друге, – зважаючи на прогнозоване пожвавлення української економіки, в умовах якого зростатимуть запити на достовірну економічну інформацію, особлива увага має бути приділена нейтралізації інформаційних загроз, ефективному відбору необхідної для вітчизняного економічного розвитку інформації. Поряд із загальносуспільним ефектом – введенням до інформаційних мереж високоякісної, актуальної інформації – розвиток цього напряму діяльності підвищить статус бібліотечних установ у суспільстві.

Крім того, очевидно, що робота бібліотечних установ у нейтралізації результатів інформаційного тероризму та хакерства шляхом якісної комплектації електронними інформаційними ресурсами своїх фондів має також бути скоординована. Така координація може бути здійснена за типом координації в банківській системі нашої держави. Ця аналогія в умовах розвитку інформаційного суспільства та зростання значення інформаційних ресурсів у житті суспільства є правомірною.

Література

1. *Кастельс М.* Інтернет – галактика / Мануель Кастельс. – Київ : Ваклер. – 2007. – С. 47.

2. *Кастельс М.* Інтернет – галактика / Мануель Кастельс. – Київ : Ваклер. – 2007. – С. 48.

3. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства : [монографія] / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – Київ, 2014. – С. 27.

4. *Тихомиров О. О.* Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки / О. О. Тихомиров // Право України: юрид. журн. 2011. – № 4. – С. 252–259.

5. *Савчук Н. В.* Кіберзлочинність: зміст та методи боротьби / Н. В. Савчук // Теоретичні та прикладні питання економіки : зб. наук. пр. – Київ : Видавничо-поліграфічний центр «Київський університет», 2009. – Вип. 19. – С. 338–342.

6. *Бабенко А. М.* Кіберзлочинність як чинник негативного впливу на криміногенну ситуацію у регіонах / А. М. Бабенко // Безпека інформації. – 2013. – № 2. – С. 112–117.

7. Чернігівщина готується до інформаційної війни з Росією [Електронний ресурс] // Чернігівська обласна державна телерадіокомпанія. – Режим доступу: http://chodtrk.com.ua/?p=16961. – Назва з екрана.

8. Опасности нападения на Мариуполь нет [Электронный ресурс] // Сегодня.ua. – 2014. – 4.09. – Режим доступа: http://www.segodnya.ua/regions/donetsk/opasnosti-napadeniya-na-mariupol-net-549684.html. – Загл. с экрана.

9. В батальоне «Донбасс» «непонятки». Никто не может понять, кто кем командует [Электронный ресурс] // SearchNews. – 2015. – 23.02. – Режим доступа: http://searchnews.info/ukraine/60888-v-batalone-donbass-neponyatki-nikto-ne-mozhet-ponyat-kto-kem-komanduet.html. – Загл. с экрана.

10. У Фейсбуці ретельно стежать за Україною, – експерт із нових медіа [Електронний ресурс] // Агенція регіональної інформації та аналітики Galinfo. – 25.02.2015. – Режим доступу: http://galinfo.com.ua/news/186381.html. – Назва з екрана.

11. Информационные войны: боты и тролли строчат без выходных [Электронный ресурс] // Новостное агентство «Харьков». – 2014. –

24.09. – Режим доступа: http://nahnews.com.ua/86928-informacionnye-vojny-boty-i-trolli-strochat-bez-vyxodnyx/. – Загл. с экрана.

12. Справа державної безпеки (нотатки з парламентських слухань «Законодавче забезпечення розвитку інформаційного суспільства в Україні») [Електронний ресурс] // З.С. – 2014. – 8.08. – Режим доступу: http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/sprava-derzhavnoji-bezpeki-notatki-z-parlamentskikh-sl/. – Назва з екрана.

13. Злодії нашого часу. В Україні зростає кількість крадіжок грошей з банківських карток [Електронний ресурс] // Корреспондент. – 2014. – 14.01. – Режим доступу: http://ua.korrespondent.net/business/financial/3284906-korrespondent-zlodii-nashoho-chasu-v-ukraini-zrostaie-kilkist-kradizhok-hroshei-z-bankivskykh-kartok. – Назва з екрана.

References

1. Kastel's, M. (2007). Internet – halaktyka [Internet – Galaxy], 47. Kyiv: Vakler [in Ukrainian].

2. Kastel's, M. (2007). Internet – halaktyka [Internet – Galaxy], 48. Kyiv: Vakler [in Ukrainian].

3. Onyshchenko, O. S., Horovyi, V. M., & Popyk, V. I. (2014). Sotsial'ni merezhi iak instrument vzaiemovplyvu vlady ta hromadians'koho suspil'stva [Social media as a tool for mutual government and civil society], 27. Kyiv [in Ukrainian].

4. Tykhomyrov, O. O. (2011). Protydiia kiberzlochynnosti iak skladova derzhavnoho zabezpechennia informatsijnoi bezpeky [Combating cybercrime as part of the state of information security]. *Pravo Ukrainy – Right Ukraine, 4*, 252–259 [in Ukrainian].

5. Savchuk, N. V. (2009). Kiberzlochynnist': zmist ta metody borot'by [Cybercrime: the content and methods of struggle]. *Teoretychni ta prykladni pytannia ekonomiky – Theoretical and Applied Economics question*, issue 19, 338–342 [in Ukrainian].

6. Babenko, A. M. (2013). Kiberzlochynnist' iak chynnyk nehatyvnoho vplyvu na kryminohennu sytuatsiiu u rehionakh [Cybercrime as a factor in the negative impact on the crime situation in the regions]. *Bezpeka informatsii – Information Security*, 2, 112–117 [in Ukrainian].

7. Chernihivschyna hotuiet'sia do informatsijnoi vijny z Rosiieiu [Chernihiv region preparing for information war with Russia]. *Chernihivs'ka oblasna derzhavna teleradiokompaniia – Chernihiv Regional State TV and Radio*

Company. chodtrk.com.ua. Retrieved from http://chodtrk.com.ua/?p=16961 [in Ukrainian].

8. Opasnosti napadenija na Mariupol' net [There is not danger of attack in Mariupol]. *segodnya.ua*. Retrieved from http://www.segodnya.ua/regions/donetsk/opasnosti-napadeniya-na-mariupol-net-549684.html [in Russian].

9. V batal'one «Donbass» «neponjatki». Nikto ne mozhet ponjat', kto kem komanduet [There are misunderstandings in the battalion «Donbass». No one can understands, who commands who]. *searchnews.info*. Retrieved from http://searchnews.info/ukraine/60888-v-batalone-donbass-neponyatki-nikto-ne-mozhet-ponyat-kto-kem-komanduet.html [in Russian].

10. U Fejsbutsi retel'no stezhat' za Ukrainoiu, – ekspert iz novykh media [Facebook carefully monitor the Ukraine – expert on new media]. *galinfo.com*. ua. Retrieved from http://galinfo.com.ua/news/186381.html [in Ukrainian].

11. Informacionnye vojny: boty i trolli strochat bez vyhodnyh [Information warfare: bots and trolls scribble without weekends]. *nahnews.com.ua.* Retrieved from http://nahnews.com.ua/86928-informacionnye-vojny-boty-i-trolli-strochat-bez-vyxodnyx/ [in Russian].

12. Sprava derzhavnoi bezpeky (notatky z parlaments'kykh slukhan' «Za-konodavche zabezpechennia rozvytku informatsijnoho suspil'stva v Ukraini») [The matter of national security (notes from the parliamentary hearings «Over-legislative provision of information society development in Ukraine»). *uaforeignaffairs.com*. Retrieved from http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/sprava-derzhavnoji-bezpeki-notatki-z-parlamentskikh-sl/ [in Ukrainian].

13. Zlodii nashoho chasu. V Ukraini zrostaie kil'kist' kradizhok hroshej z bankivs'kykh kartok [Thieves of nowadays. The number of thefts of money from bank cards are growing in Ukraine]. *ua.korrespondent.net.* Retrieved from http://ua.korrespondent.net/business/financial/3284906-korrespondent-zlodii-nashoho-chasu-v-ukraini-zrostaie-kilkist-kradizhok-hroshei-z-bankivskykh-kartok [in Ukrainian].

Стаття надійшла до редакції 17.04.2015.

Svetlana Gorovaya
V. I. Vernadsky National Library of Ukraine

Specific Library Acquisition under Activation Crime Information

The main problems associated with actualization topics of cybercrime in connection with the active development of informational and telekomunikatsiynih technologies, access to the production and use of information resources in all people, including those who are prone to delinquency in the context of what appears such a thing as hacking,

cyber-terrorism, which contributes to informational processes unlawful elements negatively affecting the development of the national information space of Ukraine.

Today, information security interests dictate the need for continuous monitoring of all sources of information production, timely response to potential threats to information related to the introduction of the public circulation of the new information. Poor information on the content, harmful and dangerous for society to influence public opinion immediately after its introduction into the system of societal communication.

With the new information modern information technologies provide opportunities for long-term impact of information on the subject of information attacks by promoting the introduction of relevant information to the database, including the library, the system informatsiynyh sovereign nation or state resources.

Accordingly, this article discusses the characteristic manifestations of cybercrime in today's information, the definition of its main threats to the information society development, for the acquisition of socially significant information resources of library collections.

Keywords: cybercrime, hackers, acquisition, information space, harmful information, library funds.

Светлана Горовая
Национальная библиотека Украины имени В. И. Вернадского

Специфика библиотечного комплектования в условиях активизации информационной преступности

Рассматриваются основные проблемы, связанные с актуализацией темы киберпреступности в связи с активным развитием информационных и телекомуникацийних технологий, доступом к производству и использованию информационных ресурсов всех категорий населения, в том числе и тех, которые склонны к правонарушениям, в контексте чего появилось такое явление как хакерство, кибертерроризм, что вносит в информационные процессы противоправные элементы, негативно влияя на развитие национального информационного пространства Украины.

Сегодня интересы информационной безопасности диктуют необходимость постоянного мониторинга всех источников информационного производства, своевременного реагирования на возможные информационные угрозы, связанные с введением в общественный оборот новой информации. Некачественная по содержанию информация, вредная и небезопасная для общества, влияет на общественное мнение сразу же после введения ее в систему существующих в обществе социальных коммуникаций.

С помощью новой информации современные информационные технологии создают широкие возможности для длительного информационного воздействия

на объект информационной атаки путем содействия введению соответствующей информации в информационные базы, в том числе библиотечные, в систему суверенных информационных ресурсов нации или государства.

В этой статье рассматриваются характерные проявления киберпреступности в условиях современной информатизации, определение ее основных угроз для информационного развития общества, для комплектования общественно значимыми информационными ресурсами фондов библиотек.

Ключевые слова: киберпреступность, хакеры, комплектования, информационное пространство, вредная информация, библиотечные фонды.