УДК 351.74/.76

С. О. Харченко
здобувач кафедри національної безпеки
(сфера прикордонної діяльності) та управління
факультету підготовки керівних кадрів
Національної академії
Державної прикордонної служби України
імені Богдана Хмельницького

НАУКОВІ ПІДХОДИ ДО КЛАСИФІКАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

У статті узагальнено наукові підходи до класифікації загроз інформаційній безпеці. Синтезовано підхід до розуміння сутності категорії «загроза інформаційній безпеці» та визначено відмінність пропонованого поняття від небезпеки в інформаційній сфері. Запропоновано авторський підхід до виділення критеріїв поділу та видів загроз інформаційній безпеці, який представлено у вигляді рубрика тора, що може розширюватись і доповнюватись залежно від потреб та специфіки діяльності конкретних установ.

Ключові слова: *загроза інформаційній безпеці, критерії поділу, види загроз інформаційній безпеці, класифікація загроз інформаційній безпеці, рубрикатор.*

Постановка проблеми. Діяльність Служби безпеки України пов'язана з функціонуванням та обігом значного обсягу таємної інформації та інформації для службового користування, несанкціонований «витік» та поширення якої можуть спричинити значні загрози національній безпеці України, її обороноздатності. Сучасний світ перетворив інформацію на своєрідний товар, що виступає об'єктом купівлі-продажу, зловживань та, в окремих випадках, об'єктом кримінальних злочинів. Така ситуація зумовлює необхідність посилення уваги до захисту інформації, яка функціонує в структурі органів Служби безпеки України, ідентифікації загроз інформаційній безпеці та їх нейтралізації.

З метою якісної ідентифікації таких загроз важливим є визначення не лише джерел їх походження, а й причин виникнення, що зумовлює необхідність їх систематизації шляхом проведення системної класифікації.

Аналіз останніх досліджень і публікацій. Окремі аспекти загроз інформаційній безпеці досліджувались у працях таких науковців, як: Берко А., Бодрука О., Бойченко О., Гуцу С., Живко З., Євдоченко Л., Кормича Б., Кузьменко Б., Євдоченко Л., Ліпкана В., Литвиненка О., Логінова А., Макарової М., Марущака А., Максименка Ю., Пилипчука В., Погребняка А. та інших.

Однак переважна частина цих праць стосується визначення сутності та загроз інформаційній безпеці, а запропоновані авторами підходи до класифікації загроз подекуди носять дискусійний характер. Крім того, в науковій літературі відсутні системні дослідження загроз інформаційній безпеці органів Служби безпеки України, що зумовлює актуальність та практичне спрямування дослідження. Теоретичне обґрунтування цього питання зумовлюється також необхідністю як оцінки рівня дієвості загроз, так і формування системи моніторингу інформаційної безпеки Служби безпеки України.

Метою статті є визначення сутності загроз інформаційній безпеці органів Служби безпеки України та розроблення наукових підходів щодо їх класифікації.

Виклад основного матеріалу. Для систематизації наукових уявлень у досліджуваній сфері необхідно передусім з'ясувати сутність терміна «загроза» та «загроза інформаційній безпеці». Так, загроза (від англ. threat) являє собою будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі. Спробу реалізації загрози називають атакою [1]. Під загрозою (взагалі) розуміють потенційно можливу подію, дію (вплив), процес або явище, які можуть спричинити шкоду чиїмось інтересам. Розглянемо погляди науковців на трактування сутності «загрози».

Так, О. Владіміров стверджує, що «загрози – це небезпеки, що реалізуються. Загрози

відбиваються. Небезпеки – це загрози, що формуються. Небезпеки відвертаються та нейтралізуються...» [2]. О. Сергунін стверджує: загроза – це «стадія крайнього загострення протиріч, безпосередній передконфліктний стан, найбільш конкретна і безпосередня форма небезпеки або сукупність умов і факторів, що ставлять під удар інтереси громадян, суспільства і держави» [3, с. 128].

Н. Різник стверджує, що загроза виникає в тому випадку, коли відбувається безпосередня дія негативних факторів впливу на стан безпеки досліджуваного об'єкта, порушуючи його рівновагу [4, с. 122].

Отже, дослідження сутності категорії «загроза» дозволяє стверджувати, що науковці досить часто вважають її похідною від поняття «небезпека». Так, якщо небезпека визначається переважно як потенційна можливість деструктивного, дестабілізуючого впливу сукупності чинників на стан об'єкта дослідження, то загрозу розуміють як реальну можливість настання негативних наслідків, тобто має місце переростання «небезпеки» в «загрозу».

Отже, загроза інформаційній безпеці є сукупністю умов і факторів, що створюють реальну небезпеку порушення інформаційної безпеки. Під загрозою інтересам суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке за допомогою впливу на інформацію або інші компоненти інформаційної системи може прямо або побічно призвести до нанесення шкоди інтересам даних суб'єктів [5].

Вважається, що безпечна система повинна володіти стійкістю до впливів, спрямованим на порушення однієї з трьох характеристик інформації, що передається, обробляється або зберігається, а саме конфіденційності, цілісності або доступності.

Під конфіденційністю (confidentiality) інформації розуміється властивість, що дозволяє відмовляти в праві на доступ до інформації або не розкривати її неповноважним особам, логічним об'єктам або процесії. Цілісність (integrity) інформації має на увазі її здатність не перетворюватись або знищуватись у результаті несанкціонованого доступу. І, нарешті, доступність (availability) інформації визначається, як її властивість бути доступною і використовуватися за запитом із боку уповноваженого користувача [6].

Саме загрозу інформаційній безпеці пов'язують із потенційною дією, спрямованою на порушення конфіденційності, цілісності і доступності інформації. Загрози інформаційній безпеці пов'язують із [7]:

– розкраданням (копіюванням) інформації;

– знищенням інформації;

– модифікацією (спотворенням) інформації;

– порушенням доступності (блокуванням) інформації;

– запереченням автентичності інформації;

– нав'язуванням неправдивої інформації.

Носіями загроз безпеці є джерела загроз. Джерелами загроз можуть виступати як суб'єкти (особистість), так і об'єктивні прояви. Всі джерела загроз безпеці можна розподілити на три основні групи [8]:

1) антропогенні джерела загроз (зумовлені діями суб'єкта);

2) техногенні джерела загроз (зумовлені технічними засобами);

3) стихійні джерела загроз.

Антропогенними джерелами загроз інформаційній безпеці виступають незалежні суб'єкти, дії яких можуть бути кваліфіковані як умисні або ненавмисні злочини. Тільки в цьому випадку можна говорити про заподіяння шкоди. Ця група найбільша і викликає найбільший інтерес з точки зору організації захисту, оскільки дії суб'єкта завжди можна оцінити, спрогнозувати і застосувати адекватні заходи. Методи протидії в цьому випадку керовані і безпосередньо залежать від волі організаторів захисту інформації.

Як антропогенне джерело загроз можна розглядати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи із системами та засобами захисту. Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації, можуть бути як зовнішні, так і внутрішні.

Зовнішні джерела можуть бути випадковими або умисними і мати різний рівень кваліфікації [9]. До них відносяться:

– кримінальні структури;

– потенційні злочинці й хакери;

– технічний персонал постачальників телематичних послуг;

– представники наглядових організацій та аварійних служб;

– представники силових структур.

Внутрішні суб'єкти (джерела), як правило, являють собою висококваліфікованих фахівців у галузі розробки й експлуатації програмного забезпечення і технічних засобів, яким відома специфіка вирішуваних завдань, структура, основні функції та принципи роботи програм-

но-апаратних засобів захисту інформації, і мають можливість використання штатного обладнання і технічних засобів мережі. До них відносяться:

– основний персонал (користувачі, програмісти, розробники);

– представники служби захисту інформації;

– допоміжний персонал (прибиральники, охорона);

– технічний персонал (життєзабезпечення, експлуатація).

Необхідно відзначити, що фахівці з безпеки вважають своїх співробітників та інших осіб, що мають доступ до внутрішньої інформації, найбільш небезпечними з точки зору загрози безпеці для їх організацій. Це є головною причиною здійснення систематичного моніторингу співробітників. До найбільш поширених методів моніторингу відносяться: моніторинг з'єднань з Інтернет (74%); вивчення всього, що безпосередньо пов'язано з роботою (62%); зберігання та читання електронних листів (43%); запис співробітників на роботі на відеокамери (18%); прослуховування телефонних розмов співробітників (12%); прослуховування повідомлень голосової пошти співробітників (7%) [10].

Особливу групу внутрішніх антропогенних джерел становлять спеціально заслані агенти. Ця група розглядається в складі перерахованих вище джерел загроз, але методи запобігання загрозам цієї групи можуть мати свої відмінності.

Друга група містить джерела загроз, які визначаються техногенною діяльністю людини і розвитком цивілізації. Цей клас джерел загроз менш прогнозований, безпосередньо залежить від властивостей технічних засобів і тому потребує особливої уваги. Технічні засоби, які є джерелами потенційних загроз безпеки, також можуть бути

зовнішніми:

– засоби зв'язку;

– мережі інженерних комунікацій (водопостачання, каналізації);

– транспорт;

і внутрішніми:

– неякісні технічні засоби обробки інформації;

– неякісні програмні засоби обробки інформації;

– допоміжні засоби (охорони, сигналізації, телефони);

– інші технічні засоби, що застосовуються в організації.

Третя група джерел загроз об'єднує обставини, які становлять непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, поширюється на всіх. До непереборної сили в законодавстві й договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти за сучасного рівня людського знання і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню, і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз, як правило, є зовнішніми відносно інформації, що захищається, і під ними насамперед розуміють природні катаклізми: (пожежі, землетруси, повені, урагани, магнітні бурі, радіоактивне випромінювання, різні непередбачені обставини, незрозумілі явища, інші форс-мажорні обставини).

Загалом, необхідно відзначити значну кількість підходів до класифікації загроз інформаційній безпеці як на національному рівні, так і в межах діяльності окремих установ та організацій. З метою систематизації загальних уявлень та агрегування підходів до виокремлення окремих видів загроз інформаційній безпеці синтезуємо результати наших досліджень у вигляді таблиці 1.

Отже, наведені підходи свідчать про наявність декількох спільних критеріїв до виділення видів загроз інформаційній безпеці: залежно від джерел походження; за властивостями інформації; за ступенем умисного впливу тощо. Також необхідно відмітити різноманітність класифікацій у чинному законодавстві, яка зумовлена не лише різноманітними підходами до вибору класифікаційних ознак та цілями класифікації, а й відсутністю належного теоретичного обґрунтування сутності загроз інформаційній безпеці.

Тому з метою узагальнення існуючих наукових поглядів щодо класифікації загроз інформаційній безпеці та визначення концептуального підходу до формулювання цього елементу пропонуємо таку розгорнуту класифікацію, яку доцільно представити у вигляді рубрикатора:

0. Загрози інформаційній безпеці

0.1. За джерелами походження загроз:

0.1.1. Антропогенні джерела загроз:

0.1.1.1.Внутрішні:

0.1.1.1.1. Основний персонал (користувачі, програмісти, розробники)

0.1.1.1.2. Допоміжний персонал (охорона, прибиральники)

0.1.1.1.3. Представники служб захисту інформації

Таблиця 1

Наукові підходи до класифікації видів загроз інформаційній безпеці

Джерело	Критерій класифікації/ види загроз інформаційній безпеці
Державний стандарт України «Захист інформації. Технічний захист інформації. Основні положення» – ДСТУ 3396.0-96 [11]	За способом впливу на інформацію: - технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали; - каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації; - несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.
Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [12]	За шляхами реалізації загроз інформаційній безпеці: - витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій; - несанкціонованих дій з інформацією, в тому числі з використанням комп'ютерних вірусів; - спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.
Державний стандарт України «Захист інформації. Технічний захист інформації. Терміни та визначення» – ДСТУ 3396.2-97 [13]	Види загроз інформаційній безпеці: - загрози витоку інформації; - загрози порушення цілісності інформації; - загрози блокування інформації.
В. Ліпкан [14]	За джерелами походження: природного походження, техногенного походження, антропогенного походження. За ступенем гіпотетичної шкоди: загроза та небезпека; За повторюваністю вчинення: повторювані та продовжувані. За сферами походження: екзогенні та ендогенні. За ймовірністю реалізації: вірогідні, неможливі, випадкові. За рівнем детермінізму: закономірні та випадкові. За значенням: допустимі та неприпустимі. За структурою впливу: системні, структурні та елементні. За характером реалізації: реальні, потенційні, здійснені, уявні. За ставленням до них: об'єктивні та суб'єктивні. За об'єктом впливу: особа; суспільство; держава.
А. Логінов [15]	Види загроз інформаційній безпеці: - розкриття інформаційних ресурсів; - порушення цілісності інформаційних ресурсів; - збій у роботі обладнання.
Б. Кузьменко, О. Чайковська [16, с. 6–7]	За властивостями інформації: - загрози порушення конфіденційності інформації, в результаті реалізації яких інформація стає доступною суб'єкту, що не володіє повноваженнями для ознайомлення з нею; - загрози порушення цілісності інформації, до яких відноситься будь-яке зловмисне спотворення інформації, оброблюваної з використанням автоматизованих систем; - загрози порушення доступності інформації, що виникають у тих випадках, коли доступ до деякого ресурсу автоматизованих систем для легальних користувачів блокується.
С. Гуцу [17] О. Литвиненко [18]	Види загроз інформаційній безпеці: - загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; - загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію та інформаційні ресурси (їх виробництво, системи формування й використання); - загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).
М. Макарова [19, с. 188].	Види загроз у мережі: - дані навмисно перехоплюються, читаються або змінюються; - користувачі ідентифікують себе неправильно (з шахрайською метою); - користувач отримує несанкціонований доступ з однієї мережі до іншої.

Таблиця 1

А. Погребняк [20, с. 46–47, 50]	Види загроз: - навмисні, до яких відносять: а) несанкціонований доступ до інформації і мережевих ресурсів; б) розкриття і модифікація даних і програм, їх копіювання; в) розкриття, модифікація або підміна трафіка обчислювальної мережі; г) розроблення і поширення комп'ютерних вірусів, уведення в програмне забезпечення логічних бомб; ґ) крадіжка магнітних носіїв і розрахункових документів; д) руйнування архівної інформації або навмисне її знищення; е) фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; є) перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку; - випадкові, які включають: а) помилки обслуговуючого персоналу і користувачів; б) втрату інформації внаслідок неправильного її збереження; в) випадкове знищення або заміну; г) збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; ґ) некоректну роботу програмного забезпечення, зокрема внаслідок зараження комп'ютерними вірусами тощо.
Вихорєв С.В. [8]	За природою виникнення: природні і штучні загрози. За ступенем навмисності: випадкові і навмисні загрози. Залежно від джерела загрози: загрози, джерелом яких є природне середовище; загрози, джерелом яких є людина; загрози, джерелом яких є санкціоновані програмно-апаратні засоби; загрози, джерелом яких є несанкціоновані програмно-апаратні засоби. Відповідно до становища джерела загрози виділяють: загрози, джерело яких розташоване поза контрольованою зоною; загрози, джерело яких розташоване в межах контрольованої зони. За ступенем впливу на автоматизовані системи: пасивні та активні загрози. За способом доступу до ресурсів автоматизованих систем: загрози, які використовують стандартний доступ; загрози, що використовують нестандартний шлях доступу.
Л. Євдоченко [21, с. 8]	За способом впливу на об'єкти інформаційної безпеки: інформаційні, фізичні й програмно-математичні, організаційно-правові. За джерелами надходження: внутрішні та зовнішні. За характером вияву: політичні, економічні, організаційно-технічні.

Джерело: систематизовано автором

0.1.1.1.4. Шпигуни
0.1.1.2. Зовнішні:
0.1.1.2.1. Кримінальні структури
0.1.1.2.2. Хакери
0.1.1.2.3. Технічні працівники постачальників телематичних послуг
0.1.1.2.4. Силові дії (теракт, збройний конфлікт)
0.1.1.2.4. Представники аварійних служб
0.1.1.2.5. Представники силових структур
0.1.2. Техногенні джерела загроз:
0.1.2.1.Внутрішні:
0.1.2.1.1. Технічні прилади для обробки інформації
0.1.2.1.2. Програмні засоби обробки інформації
0.1.2.1.3. Допоміжні засоби (сигналізації, охоронна система)
0.1.2.1.4. Інші технічні засоби
0.1.2.2. Зовнішні:
0.1.2.2.1. Засоби зв'язку
0.1.2.2.2. Мережі інженерних комунікацій
0.1.2.2.3. Транспорт
0.1.3.Стихійніджерелазагроз(форс-мажорні):
0.1.3.1. Пожежі
0.1.3.1. Землетруси
0.1.3.1. Повені
0.1.3.1. Урагани
0.1.3.1. Магнітні бурі
0.1.3.1. Радіоактивне випромінювання
0.1.3.1. Інші непередбачувані події
0.2. За способом впливу на інформацію:
0.2.1. Технічними каналами
0.2.2. Каналами спеціального впливу
0.2.3. Несанкціонованим доступом
0.3. За способом викривлення інформації:
0.3.1. Витік інформації
0.3.2. Порушення цілісності інформації
0.3.3. Спотворення інформації
0.3.4. Блокування інформації
0.4. За ступенем умисності впливу:
0.4.1. Ненавмисні (випадкові)
0.4.2. Умисні
0.5. За ступенем інтенсивності впливу:
0.5.1. Активні
0.5.2. Пасивні
0.6. За ступенем контрольованості:
0.6.1. Контрольовані
0.6.2. Неконтрольовані
0.6.3. Частково контрольовані
0.7. За ступенем передбачуваності:
0.7.1. Передбачувані

0.7.2. Непередбачувані

0.7.3. Частково передбачувані

Запропонована форма представлення класифікації загроз інформаційній безпеці за необхідності може розширюватись та доповнюватись у вузлах «дерева» рубрикатора.

Висновки і пропозиції. Таким чином, проведена систематизація наукових підходів до класифікації загроз інформаційній безпеці свідчить про наявність безлічі класифікаційних критеріїв та видів досліджуваних загроз. Самі ж загрози інформаційній безпеці визначаються високою ймовірністю заподіяння шкоди, що завдається організації, в разі порушення цілісності її інформаційної системи. На основі повної системи класифікації можна оцінити як збиток, викликаний порушенням інформаційної безпеки, так і витрати на захист від загроз її порушення, а аналіз ризиків дозволить спланувати заходи щодо визначення того, які ресурси і від яких загроз треба захищати, а також в якому ступені ті або інші ресурси потребують захисту.

Список використаної літератури:

1. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.
2. Владимиров А. «Вызовы», «риски», «опасности», «угрозы», «кризисы», «катастрофы» и «крах» как важные категории политологии и теории войны. URL: http://www.kadet.ru/lichno/vlad_v/ Ocenka_riskov.htm.
3. Сергунин А.А. Международная безопасность: новые подходы и концепты. *Политические исследования.* 2005. № 6. С. 126–137.
4. Різник Н.С. Теоретичні засади формування системи діагностики економічної безпеки банку. *Вісник Харк. нац. техн. ун-ту сільського господарства : Економічні науки.* Харків : ХНТУСГ, 2007. Вип. 66. С. 118–123.
5. Крат Ю.Г., Шрамкова Т.Г. Основы информационной безопасности : учеб. пособие. Хабаровск : Изд-во ДВГУПС, 2008. 112 с.
6. Эрик С. Реймонд. Новый словарь хакера. Москва, 1996. 262 с.
7. Вакка Дж. Безопасность интранет. Москва, 1998. 496 с.
8. Вихорев С.В. Классификация угроз информационной безопасности. URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml.
9. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. Москва, 2000. 448 с.
10. 2017 CSI/FBI Computer Crime and Security Survey Continue but Financial Losses are Down. URL: http://i.cmpnet.com/ gocsi/db_area/pdfs/fbi/FBI2017.pdf.
11. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. Чинний від 01.01.1997 р. URL: www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38883&cat_id=38836.
12. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.06 р. № 373. *Офіційний вісник України.* 2006. № 13.
13. Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. Чинний від 1998.01.01. URL: www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38934&cat_id= 38836.
14. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції. URL: www.pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi.
15. Логінов А.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. на здобуття наукового ступеня кандидата юридичних наук : 12.00.07 ; Національна академія внутрішніх справ України. Київ, 2005.
16. Кузьменко Б.В., Чайковська О.А. Захист інформації : навч. посіб. Ч. 2. Київ : Видавничий відділ КНУКіМ, 2009. 69 с.
17. Гуцу С.Ф. Правові основи інформаційної діяльності. Чайковська Чайковська. URL: http://studrada.com.ua
18. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. URL: www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf.
19. Макарова М.В. Електронна комерція : посібник для студентів вищ. навч. закладів. Київ : Видавничий центр «Академия», 2002. 272 с.
20. Погребняк А.В. Технології комп'ютерної безпеки : монографія. Рівне : МЕГУ, 2011. 117 с.
21. Євдоченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр. : 25.00.01 / Л.О. Євдоченко. – Л., 2011. – 24 с.

Харченко С. О. Научные подходы к классификации угроз информационной безопасности

В статье обобщены научные подходы к классификации угроз информационной безопасности. Синтезирован подход к пониманию сущности категории «угроза информационной безопасности» и определено отличие предлагаемого понятия от опасности в информационной сфере. Предложен авторский подход к выделению критериев разделения и видов угроз информационной безопасности, который представлен в виде рубрикатора и может расширяться, дополняться в зависимости от необходимости и специфики деятельности конкретных учреждений.

Ключевые слова: *угроза информационной безопасности, критерии разделения, виды угроз информационной безопасности, классификация угроз информационной безопасности, рубрикатор.*

Kharchenko S. O. Scientific Approaches to the Classification of Threats to Information Security

The article summarizes the scientific approaches to the classification of threats to information security. The approach to understanding the essence of the category “the threat to information security” has been synthesized. The difference between the proposed concept and the threat in the information sphere has been determined. The author's approach to distinguishing the criteria and the types of threats to information security has been proposed. It is presented as a rubricator that can be expanded and supplemented depending on the necessity and specific features of the activities of the institutions.

Key words: *threat to information security, criteria to distinguish, types of threats to information security, classification of threats to information security, rubricator.*