УДК 007:351.778.542

О. О. Ільїн, С. О. Сєрих, В. В. Вишнівський

АНАЛІЗ УРАЗЛИВОСТІ ІНФОРМАЦІЙНОГО РЕСУРСУ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ ТА КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

З метою синтезу системної моделі порушника інформаційної безпеки проведено аналіз уразливості інформаційних ресурсів Вищих навчальних закладів в Україні. Розглянути можливі загрози та причини їх виникнення, методи забезпечення захисту інформації. Для формування дієвої системи моніторингу та управління в сфері інформаційної безпеки Вищого навчального закладу, а також вдосконалення відповідної нормативно-правової бази наведено класифікацію загроз та напрямки управління інформаційними ризиками закладів.

Ключові слова: інформаційний ресурс, інформаційна технологія управління, уразливість, ризики, когнітивна модель, моделі загроз, модель порушника, модель реалізації загроз, захист інформаційного ресурсу.

Постановка проблеми. Характерною ознакою сучасного етапу науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх використання у повсякденному житті. Наявність і доступність високотехнологічного обладнання, створення глобальних інформаційно-телекомунікаційних мереж, інтеграція інформаційних систем наукових закладів з метою раціонального використання інформаційного ресурсу (ІР) сприяють інтенсифікації роботи науково-педагогічних і інших працівників Вищих навчальних закладів та покращують учбовий процес, який все частіше набуває ознак дистанційного навчання.

Разом з тим неконтрольований доступ до інформаційного ресурсу Вищого навчального закладу, стан інформаційної безпеки (ІБ), низька захищеність від зовнішніх та внутрішніх загроз мають негативні наслідки – ризик порушення цілісності, доступності та конфіденційності інформації.

Удосконалення управління інформаційними ризиками складна задача, яка потребує глибокого дослідження загроз ІБ, джерела та причин їх виникнення, оцінки рівня уразливості ІР учбового закладу, що в свою чергу дозволить здійснити синтез моделі порушника ІБ та в подальшому когнітивної моделі управління ризиками. Тому актуальність теми є очевидною, оскільки система ІБ відображає стан захищеності інтересів не тільки студентів і викладачів, а і національних інтересів країни, бо останні проводять крім навчальної ще і наукову роботу.

Аналіз останніх досліджень і публікацій. Варто зазначити, що питання пов’язані з темою дослідження зустрічаються в працях: А. Ю. Берко, М.Б. Левицької, В.А. Ліпкана, Б.А. Кормича, В.М. Лопатіна, Ю.Є. Максименко, А.І. Марущака, Г.В. Новицького та інших. Проте, не зважаючи на значний рівень наукового осмислення проблем інформаційної безпеки, питання загроз, зокрема їх класифікації, продовжують мати дискусійний характер, що додатково обумовлює актуальність статті.

Мета статті. Головною метою роботи є теоретичне обґрунтування інформаційної безпеки Вищих навчальних закладів, виявлення загроз та напрямків вдосконалення управління інформаційними ризиками навчальних закладів, аналіз уразливості інформаційних ресурсів та класифікація загроз з метою пошуку та надання оптимальних засобів, які дозволяють забезпечити створення стійкої системи їх інформаційної безпеки.

Виклад основного матеріалу дослідження. Аналіз уразливості інформаційного ресурсу Вищого навчального закладу та їх наслідки в повній мірі відповідають таким негативним проявам, які притаманні іншим закладам и установам держави [1], це збільшення фактів протизаконного збору і використання інформації, несанкціонованого доступу і використання ІР, незаконного копіювання інформації, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікації даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку. Разом з тим для Вищих навчальних закладів є і особливості, що пов’язані із блокуванням доступу до відкритої інформації при дистанційному навчанні,

введення хибних теоретичних і оціночних даних, ведення електронного діалогу від особи викладача.

У Державному стандарті України „Захист інформації. Технічний захист інформації. Основні положення.” ДСТУ 3396.0-96 формулювання класифікації загроз відсутнє, проте передбачено можливі шляхи їх реалізації [2], що дозволяє визначити ймовірні загрози і ввести різні класіфікаційні ознаки їх проявів в ІБ.

Так в [3] з метою узагальнення поглядів щодо класифікації загроз ІБ пропонуються таки признаки: 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. Але збільшення ознак не гарантує практичного розв’язання проблем підвищення ІБ для Вищих навчальних закладів, бо не дозволяє синтезувати системну модель порушника інформаційної безпеки і локалізувати місця доступу до ІР. А це в свою чергу визначити інформаційні ризики для здійснення оптимізації управління ними.

Оскільки організація забезпечення ІБ повинна носити комплексний характер і ґрунтуватися на аналізі уразливості ІР та негативних наслідків, то потрібна ідентифікація можливих джерел загроз, факторів, що сприяють їх прояву, що для моделювання доцільно проводити на основі аналізу наступного логічного ланцюжка (рис.1).

Рис.1. Логічний ланцюг аналізу уразливості ІР

Джерела загроз – це потенційні антропогенні, техногенні та природні загрози ІБ, де під самою загрозою (в цілому) розуміють потенційно можливу подію, вплив, процес або явище, яке може привести до нанесення збитку інтересам суб'єктів та стану об’єктів інформаційних систем (ІС), їх інформаційним відносинам, яке за допомогою впливу на інформацію або інші

компоненти ІС може прямо або опосередковано призвести до нанесення шкоди інтересам даних суб'єктів.

Уразливість – це притаманні об'єкту ІС причини, що призводять до порушення ІБ на конкретному об'єкті і обумовлені недоліками процесу функціонування об'єкта системи, властивостями її архітектури, протоколами обміну і інтерфейсами, застосованого програмного забезпечення і апаратної платформи, умовами експлуатації, неуважністю співробітників.

Наслідки – це можливі дії реалізації загрози при взаємодії джерела загрози через наявні уразливості. В наслідках саме збитки підлягають чисельним розрахункам втрати часу чи фінансовим затратам на відновлення. Тому до класифікаційної ознаки загроз обов'язково слід віднести такі наслідки:

- розкрадання (копіювання інформації);
- знищення інформації;
- модифікація (спотворення) інформації;
- порушення доступності (блокування) інформації;
- заперечення достовірності інформації;
- нав'язування неправдивої інформації.

На кінцевий результат найбільш впливова початкова ознака – джерела загроз, які доцільно поділити на три групи.

1. Антропогенні джерела – ті, що обумовлені діями суб'єкта, які можуть призвести до порушення безпеки інформації. Такі дії можуть бути кваліфіковані як навмисні або випадкові, а за адміністративно-правовими відносинами – злочинними. Незалежно від приналежності та місця джерела при розподілі їх на зовнішні і внутрішні їх можливо і доцільно прогнозувати, а отже планувати, закладати в ризики і вживати адекватних заходів для зменшення уразливості ІС.

2. Техногенні джерела, обумовлені технічними засобами. Ці джерела загроз менш і складніш прогнозуються, безпосередньо залежать від властивостей техніки, структури і архітектури мереж Вищого навчального закладу, наявності ліцензійного ПЗ і додаткових програм захисту інформації, кваліфікації адміністраторів мереж та обслуговуючого персоналу, тому вимагають особливої уваги. Дані джерела загроз ІБ, також можуть бути як внутрішніми, так і зовнішніми, а для синтезу їх моделі і оцінки ризиків [4] раціонально використовувати когнітивні моделі оцінки.

3. Стихійні джерела – група об'єднує обставини, що становлять непереборну силу (стихійні лиха, або ін. обставини, які неможливо передбачити або запобігти чи можливо передбачити, але неможливо запобігти), такі обставини, які носять об'єктивний і абсолютний характер, поширюється на всіх. Такі джерела загроз не піддаються прогнозуванню і тому заходи проти них повинні застосовуватися завжди. Стихійні джерела, як правило, є зовнішніми по відношенню до захищеного об'єкта і під ними, як правило, розуміються природні катаклізми. Для зменшення часу на відновлення самим дієвим засобом залишається резервування обладнання і ПЗ, добове чергування, постійний моніторинг тощо.

Територіально розподілена, частіше кампусна структура інформаційної системи Вищих навчальних закладів, за визначенням повинна бути відкритою, тому створює ряд передумов для реалізації різноманітності потенційних загроз ІБ, що можуть завдати шкоди всім складовим ІС. Різноманітність настільки значна, а випадковість появи атак, мета їх застосування і оснащеність стрімко зростає, що це не дозволяє передбачити кожну загрозу. Тому аналізуючи характеристики загроз треба вибирати протидії з позицій здорового глузду, одночасно виявляючи не тільки самі загрози, розмір потенційного збитку, але і поєднувати окремі випадки застосувань в підгрупи джерел і зменшувати загальну уразливість системи та застосовувати принцип диференціації рівня захисту на основі оцінювання ризиків.

Так за результатами практичного моделювання [5] для створеної модель навчально-методичного відділу Вищого навчального закладу із використанням всіх типів загроз здатними завдати шкоди інформаційній системі отримані таки результати. Рівень збитку

42,3%, рівень ризику 9,6%. При цьому застосування мір захисту дозволило отримати наступні результати:

– застосування політика безпеки (невиконані вимоги-21,1%, ризик-23%);
– використання організаційних заходів (невиконані вимоги-37,5%, ризик-35%);
– управління ресурсами (невиконані вимоги-18,2%, ризик-12,7%);
– помилка і безпека персоналу (невиконані вимоги-13,3%, ризик-12,6 %);
– фізична безпека обладнання і ліній зв'язку (невиконані вимоги-26%, ризик-23 %).

Загальний рівень збитків досягає 42 %, а це значне порушеннях рівноваги ІС і відчутна шкода. Уваги слід приділити удосконаленню організаційних мір захисту, що складають найбільші ризики.

Тоді доцільно запропонувати модель реалізації загроз ІБ, яка представлена на рис.2.

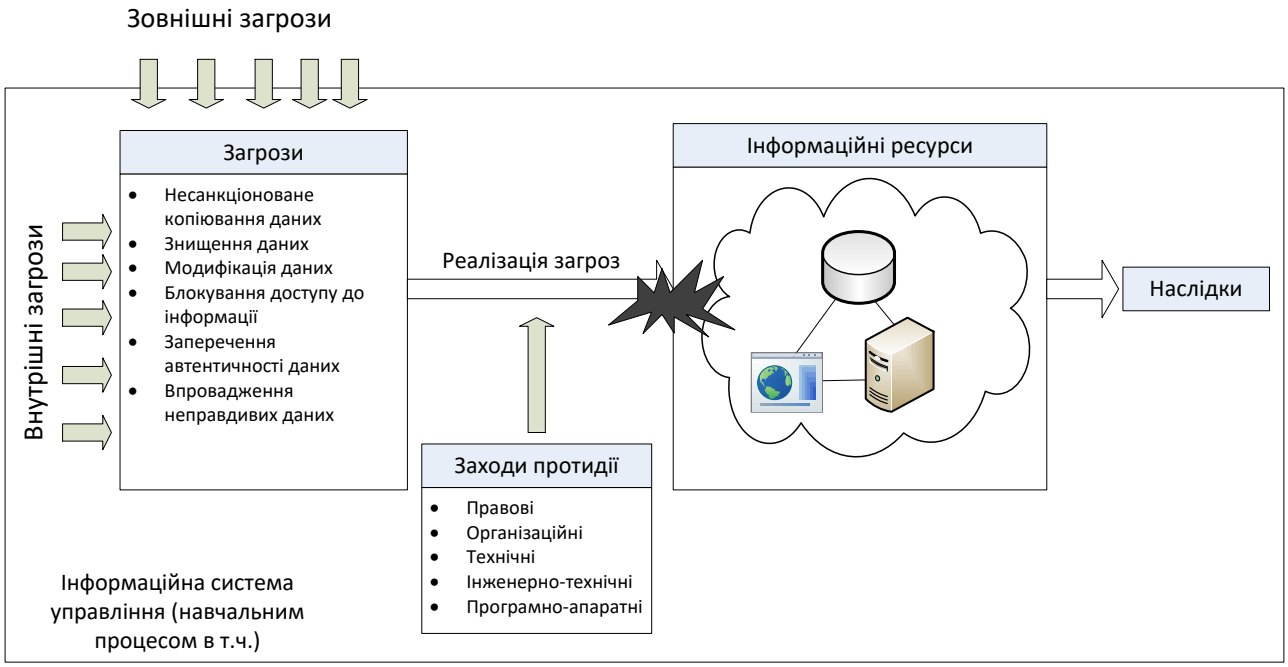

Рис.1. Модель реалізації загроз ІБ

Центральний маршрутизатор пов'язаний з локальними мережами корпусів Вищого навчального закладу за допомогою проводових ліній зв'язку. Через корпусні маршрутизатори здійснюється зв'язок з комутаторами кафедр та інших підрозділів вузу. Доступ в Інтернет здійснюється через центр інформаційних технологій (ЦІТ). Деякі комп'ютери мережі можуть мати зовнішні IP-адреси, що робить їх доступними через Інтернет, минаючи ЦІТ. Інформаційна інфраструктура вузу може бути представлена у вигляді ієрархії наступних основних рівнів:

– фізичного (лінії зв'язку, апаратні засоби тощо);
– мережевого (мережеві апаратні засоби, маршрутизатори, комутатори тощо);
– мережевих додатків і сервісів;
– операційних систем (ОС);
– систем управління базами даних (СУБД);
– технологічних процесів і додатків;
– бізнес-процесів Вищого навчального закладу.

Кожний рівень та елемент може бути об'єктом атаки, особливо коли поєднання здійснюється за безпроводовою технологією, що потребує прорахунку показників ІБ мережі ще на етапі її проектування, а на етапі експлуатації постійного моніторингу та обліку використання її інформаційних ресурсів.

Класифікація за ознакою «мета використання загроз» отримана на основі аналізу і за якою запропонована Доктрина інформаційної безпеки України [6] показує, що на першому місці по частоті виникнення стоять крадіжки інформації (65,8%), на другому місці - недбалість співробітників (55,1%), на третьому - вірусні атаки (41,7%)). Співвідношення внутрішніх і зовнішніх загроз становить відповідно 43,5 і 56,5%. У категорію внутрішніх загроз були віднесені недбалість співробітників, саботаж і фінансове шахрайство, у категорію зовнішніх загроз — дія вірусів, хакерів і спаму. Найбільш небезпечною внутрішньою загрозою ІБ виявилася витік конфіденційної інформації, що чинена інсайдерами (70%). Найбільший збиток при цьому пов'язаний з фінансовими збитками (46%), далі йдуть — погіршення іміджу і громадської думки (42,3%), втрата клієнтів (36,9%). Необхідно підкреслити, що отриманий загальний спектр загроз і тенденцій їх розвитку характерний і для освітніх установ.

Тоді модель порушника ІБ повинна відображати причини і мотиви його дій, його можливості, апріорні знання, мету дій, їх пріоритетність, шляхи досягнення (способи реалізації вихідних загроз, місце і характер дії, можливу тактику, мотиви поведінки). Взагалі це може бути декілька моделей дій зловмисника, що відображають різний рівень його підготовленості, що пояснює розподіл джерел за ознакою – категорія порушника ІБ.

Для Вищого навчального закладу типовими категоріями стають ті, що приймають участь в життєдіяльності закладу, суттєво впливають на стан ІБ, мають наступні характеристики і оцінки.

Студент. Загрози з боку студентів йдуть по декількох напрямках. По-перше, це неконтрольований вихід в Інтернет, що тягне за собою різке збільшення трафіку і нецільове витрачання IP, а нелегальне скачування до зараження вірусами мережі, що відповідно призводить до обмеження доступу великого контингенту студентів і викладачів або навіть повного блокування мережі.

По-друге, Вищий навчальний заклад - це місце підвищеної активності і концентрації хакерів-початківців. Юнацький максималізм, бажання випробувати свої знання і справити враження на однокурсників спонукає студентів зламати мережу, заблокувати вихід в Інтернет, отримати адміністративний доступ, влаштувати вірусну епідемію або вчиняти інші комп'ютерні правопорушення. Це веде до зриву занять або блокування доступу до мережі.

По-третє об’єктивна зміна життєвих цінностей і різке збільшення кількості студентів на комерційній основі вносить певні труднощі в забезпечення безпеки самого навчального процесу, бо застосовується:

– широке використання в студентському середовищі сучасних інфокомунікаційних технологій для складання заліків та іспитів (ноутбуки, планшети, смартфони із бездротовим доступом до Інтернету);

– підробки залікових і екзаменаційних відомостей, залікових книжок, відпрацювання та захисту практичних і лабораторних занять, курсових робіт;

– плагіат на стадії виконання рефератів, курсових робіт і проектів тощо.

До четвертого напрямку загроз відносяться можливі розкрадання, в тому числі, комп'ютерного обладнання та бібліотечного фонду. Тут втрати мають суто матеріальний характер, пов'язаний з необхідністю відновлення ресурсів.

І останній напрям загроз - це ненавмисні помилки студентів, що має наслідки виходу з ладу обладнання, зриву занять, обмеження доступу інших користувачів до інформації.

Співробітник. Серед загроз з боку співробітників Вищого навчального закладу, можна виділити такі:

1. В області відкритої інформації - це неправомірне використання веб-доступу, так як практично всі кафедри, викладачі та співробітники мають вільний, слабо контрольований доступ в Інтернет.

2. В області конфіденційної інформації, що має характер службової таємниці, - це витік, розголошення, модифікація інформації, що може нанести шкоду діяльності чи іміджу закладу.

3. В області комерційної інформації — привласнення чужої інтелектуальної власності або передачу їх третім особам.

4. Халатність і безвідповідальність співробітників, що тягне за собою реалізацію загроз і пов'язаний з цим збитків;

5. Ненавмисні помилки при роботі з обчислювальною технікою, так як не всі співробітники мають відповідну кваліфікацію.

Відвідувач. Дана категорія осіб практично не має фізичного доступу до інформаційної системи Вищого навчального закладу. Можливості їх обмежені, вони можуть здійснювати тільки поодинокі дії, скориставшись недбалістю або безвідповідальністю працівників, однак збиток від їх дій може бути істотним.

Хакер-одинак. Використовує стандартні комп'ютерні програми для реалізації відомих вразливостей. Це може бути і студент, що має доступ як з середини мережі, так і віддалений доступ. Дії його носять експериментальний характер, фінансова мотивація - не головне. Йому цікаво зламати сайт, отримати доступ до конфіденційної інформації, до серверів організації, до систем адміністрування, контролю і управління інформаційною системою. Дії його можуть завдати шкоди цілісності мережі. Найчастіше його дії носять несистемний характер, і він зупиняється після першого успішно проведеного злому. У той же час, він може мати і чисто матеріальний інтерес, розраховуючи на підключення та використання каналів зв'язку з високою пропускною здатністю.

Хакерська трупа - переслідує суто матеріальний інтерес. Володіючи достатніми сумарними знаннями в області комп'ютерних технологій, такі зловмисники можуть організувати сканування інформаційної системи Вищого навчального закладу з метою виявлення нових вразливостей, самостійно написати програми для експлуатації цих вразливостей. Вони діють цілеспрямовано і можуть отримати доступ до різних фінансовим документів, влаштувати потужні атаки на інформаційну систему з повним виводом її з ладу, що може завдати істотної матеріальної шкоди закладу.

Конкуренти. Підвищилася в останні роки конкуренція між вузами за надання освітніх послуг, це змушує окремо виділити цю групу порушників. Разом з тим в рамках Вищого навчального закладу нерідко проводяться дослідницькі та дослідно-конструкторські розробки за договорами з різними підприємствами країни, зарубіжними організаціями, а також вигранних грантів. У закладах існують відділи інтелектуальної власності, які проводять роботу по закріпленню інтелектуальної власності розробок та на договірних засадах обслуговує інші фірми. Дії конкурентів можуть носити як прихований, так і відкритий, демонстративний характер. Конкуренти можуть вживати серйозні зусилля за отримання відомостей, що становлять комерційну таємницю, відомостей щодо функціонування інформаційної системи Вищого навчального закладу, використовуючи для цього підкуп співробітників. Конкуренти мають свої потужні обчислювальні мережі, штат кваліфікованих співробітників в області IT-технологій і достатні фінансові кошти для здійснення протиправних дій.

Злочинні угрупування і організації. Вищі навчальні заклади виконують важливу соціально роль, спрямовану на виховання молоді, де зосереджена велика кількість людей у віці від 17 до 23 років. Тому заклади, стають мішенню для дії злочинних угруповань та організацій для проведення різних терористичних актів, поширення наркотиків і завоювання впливу на молоді незміцнілі уми з боку різних політичних партій, екстремістських угруповань і релігійних сект. Ця група зловмисників представляє серйозну загрозу як для закладу в цілому, так і для його інформаційного середовища. Залежно від цілей, подібні організації можуть мати досить високий фінансовий потенціал і підготовлених фахівців.

Висновки

Проведений аналіз основних джерел загроз і дій зловмисників, характерних для інформаційної системи Вищого навчального закладу, показує, що до них належать, насамперед, внесення вірусів у мережу університету; атаки на персональні дані

співробітників і студентів; привласнення чужої інтелектуальної власності; підробка результатів рубіжного контролю знань студентів; несанкціоноване використання ресурсів Інтернет; збої комп'ютерів і ПЗ; атаки з боку конкурентів.

Заходи захисту інформації (протидії) від таких джерел повинні ретельно продумуватися, до них можна віднести:

– Правові (закони, статути, накази, постанови);

– Організаційні (розробка і затвердження функціональних обов'язків посадових осіб служби ІБ; фізичний контроль доступу; розробка правил управління доступом до ресурсів системи; явний і прихований контроль за роботою персоналу; проведення регулярних семінарів, спецкурсів для адміністраторів мереж Вищого навчального закладу, з метою забезпечення відповідності рівня знань сучасним вимогам);

– Технічні (передбачається наявність методик визначення загроз та каналів витоку інформації і знання засобів добування (зняття) інформації);

– Інженерно-технічні (забезпечують унеможливлення несанкціонованого доступу сторонніх осіб на об'єкти захисту)

– Програмно-технічні (методи ідентифікації і аутентифікації користувачів; реєстрація дій користувачів; засоби захисту від НСД, міжмережеві екрани);

Список способів протидії повинен, у разі необхідності поповняться новими засобами захисту. Це необхідно для підтримки системи безпеки закладу в актуальному стані.

Проведений аналіз уразливості інформаційних ресурсів Вищих навчальних закладів в Україні надає можливість здійснення синтезу повної системної моделі порушника ІБ, а на її основі модель управління інформаційними ризиками навчальних закладів задля формування дієвої системи моніторингу та управління в сфері інформаційної безпеки Вищи навчальних закладів, а також вдосконалення відповідної їх нормативно-правової бази.

Література

1. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук. : спец. 12.00.01 / Максименко Ю. Є. – К., 2007. – 22 с.

2. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – [Чинний від 1997.01.01]. – [Електроний ресурс] / Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України.– Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid =5D34EDB7C.

3. Ліпкан В.А. Національна безпека України [Електронний ресурс]. – Режим доступу: http://pidruchniki.ws/15341220/politologiya/ponyattya_vidi zagroz natsionalnim interesam natsionalniy bezpetsi_informatsiyniy_sferi.

4. Берко А. Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / Берко А. Ю., Висоцька В. А., Рішняк І. В. // Вісник Національного університету "Львівська політехніка". – 2008. – № 610. – С. 20–33.

5. Фендрикова Е. И., Белов И. В., Моисеев В. В. Исследование модели угроз информационной системе для учебно-методического управления вуза в Digital Security Office // Молодой ученый. — 2014. — №6. — С. 122-125.

6. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : Офіційне Інтернет-представництво Президента України http: // www.president.gov.ua

Надійшла 22.02.2017 р. Рецензент: д.т.н., проф. Чичикало Н.І.