УДК 004.056

Колісниченко М.А., студентка групи 125м-16-1,
Науковий керівник: Тимофєєв Д.С., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

Інформаційна безпека ВНЗ України

У наш час в умовах загальної інформатизації та розвитку інформаційних технологій посилюються загрози національній безпеці України в інформаційній сфері.

Концепцію національної безпеки України стосовно інформаційної сфери розвиває Доктрина інформаційної безпеки України .

Доктрина інформаційної безпеки визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [1]. У Доктрині зазначено, що забезпечення інформаційної безпеки України грає ключову роль в забезпеченні національної безпеки України. Слід відмітити, що одним із пріоритетних напрямків державної політики в галузі забезпечення інформаційної безпеки України є розвиток освіти в області інформаційної безпеки та вдосконалення підготовки кадрів. Особливу роль у вирішенні цих завдань відіграють вузи.

Система вищої освіти України перебуває у процесі постійного вдосконалення, що зумовлено трансформаційними змінами в суспільстві. Українська вища школа переживає період адаптації не тільки до об'єктивних процесів інформаційного суспільства, а й до нових соціально-політичних умов з різноплановими проявами конкурентної боротьби.

На сьогоднішній день створення ефективних механізмів управління інформаційними ресурсами системи вищої освіти в сучасних умовах неможливо без наукового обґрунтування та практичної реалізації збалансованої політики інформаційної безпеки вузу, яка може бути сформована на основі вирішення наступних завдань [2] :

− аналіз процесів інформаційної взаємодії в усіх сферах основної діяльності українського технічного вузу: інформаційних потоків, їх масштабу і якості, протиріч, конкурентної боротьби з виявленням власників і суперників;

− розробка якісного і кількісного опису інформаційної взаємодії;

− введення кількісних індикаторів і критеріїв відкритості, безпеки і справедливості інформаційного обміну;

− розробка сценаріїв необхідності і значущості балансу в інформаційній відкритості і конфіденційності;

− визначення ролі і місця політики інформаційної безпеки в управлінні інформаційними ресурсами вузу і створення узгоджених принципів і підходів;

− формулювання основних складових політики: цілей, завдань, принципів і ключових напрямків забезпечення інформаційної безпеки;

− розробка базових методик управління процесом забезпечення політики інформаційної безпеки;

− підготовка проектів нормативно-правових документів.

У сьогочасному вузі зберігається і обробляється величезна кількість різних даних, які пов'язані не тільки із забезпеченням навчального процесу, а й з науково-дослідними та проектно-конструкторськими розробками, персональні дані студентів і співробітників, службова, комерційна та інша конфіденційна інформація.

ВНЗ являє собою публічний заклад з непостійною аудиторією, а також є місцем підвищеної активності «початківців кіберзлочинців», у цьому і полягає специфіка захисту інформації в освітній системі .

Основними загрозами безпеки інформації у вузі можуть бути:

- спроби несанкціонованого адміністрування баз даних;
- дослідження мереж, несанкціонований запуск програм з аудиту мереж;
- видалення інформації, в тому числі бібліотек;
- запуск ігрових програм;
- установка вірусних програм і троянських коней;
- спроби злому АС «ВНЗ»;
- сканування мереж, в тому числі інших організацій, через Інтернет;
- несанкціонована відкачка з Інтернету неліцензійного софту і установка його на робочі станції;
- спроби проникнення в системи бухгалтерського обліку;
- пошук «дірок» в ОС, firewall, Proxy-серверах;
- спроби несанкціонованого віддаленого адміністрування ОС;
- сканування портів і т. п.

Особливості вузу як об'єкта інформатизації пов'язані також з багатопрофільним характером діяльності, великою кількістю форм і методів навчальної роботи, просторовим розгалуженням інфраструктури (філії, представництва). Сюди ж можна віднести і різноманіття джерел фінансування, наявність розвиненої структури допоміжних підрозділів і служб (будівельна, виробнича, господарська діяльність), необхідність адаптації до мінливого ринку освітніх послуг, потреба в аналізі ринку праці, відсутність загальноприйнятої формалізації ділових процесів, необхідність електронної взаємодії з вищестоящими організаціями, часта зміна статусу співробітників і учнів.

У результаті зростання кількості злочинів у сфері інформаційних технологій з'являється велика кількість вимог до захисту ресурсів обчислювальних мереж навчальних закладів і виникає потреба у постановці завдання побудови власної інтегрованої системи безпеки. Її рішення припускає наявність нормативно-правової бази, формування концепції безпеки, розробку заходів, планів і процедур щодо безпечної роботи, проектування, реалізацію і супровід технічних засобів захисту інформації в рамках освітнього закладу. Ці складові визначають єдину політику забезпечення безпеки інформації в вузі.

На жаль, роботи по кожному з перерахованих елементів носять фрагментарний характер і пов'язано це з:

- недостатнім фінансуванням робіт із захисту інформації;
- відсутністю єдиної політики інформаційної безпеки вузів, регіональних органів та самого міністерства освіти ;
- відсутність у адміністрації освітніх установ чітких уявлень про те, що саме і як необхідно захищати.

Можна зробити висновок, що тільки комплексна робота усіх складових процесу управління інформаційною безпекою ВНЗ може привести до створення безпечного інформаційного освітнього середовища.

ПЕРЕЛІК ПОСИЛАНЬ

1. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017 [Електронний ресурс] .- Режим доступу: http://www.president.gov.ua/documents/472017-21374

2. Труфанов А. И. Политика информационной безопасности вуза как предмет исследования // Проблемы Земной цивилизации. – Вып. 9. – Иркутск: ИрГТУ, 2004 [Електронний ресурс] .- Режим доступу: / library.istu.edu/civ/default.htm.