УДК 681.513:37:65.012

О.К. Юдін, доктор технічних наук, професор,
С.С. Кривша, аспірант, А.С. Супрунов, аспірант
(Національний авіаційний університет, Україна)

КОНЦЕПТУАЛЬНІ ПИТАННЯ СТАНДАРТИЗАЦІЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Авторами досліджено загально-концептуальні питання побудови і впровадження КСЗІ інформаційних ресурсів ВНЗ України, а також розглянуто та визначено основні проблеми, що пов'язані з стандартизацією побудови КСЗІ інформації вищого навчального закладу з урахуванням міжнародних та державних стандартів.

Вступ. Зростання міжнародного рейтингу України за рахунок розвитку інтелектуального потенціалу держави є одним із пріоритетних напрямів внутрішньої політики в наш час. Основним рушієм даного процесу є ефективна система освіти та науки, яка здатна забезпечити державу сучасними технологіями та кваліфікованими фахівцями всіх сфер життєдіяльності країни. Впровадження інформаційних технологій в освіту призвело до нових загроз не лише для конфіденційної інформації, що циркулює в інформаційних системах вищих навчальних закладів (ВНЗ), але й для неперервності процесу якісної освіти та інноваційно-творчої і наукової діяльності.

У сучасному вищому навчальному закладі зберігається і обробляється величезна кількість різних даних, пов'язаних не тільки із забезпеченням навчального процесу, але й з науково-дослідними та проектно-конструкторськими розробками, персональні дані студентів і співробітників, службова, комерційна та інша конфіденційна інформація.

Постановка задачі. Зростання кількості злочинів у сфері високих технологій диктує свої вимоги до захисту ресурсів обчислювальних мереж навчальних закладів і ставить завдання побудови власної інтегрованої системи безпеки. Саме вирішення цього завдання потребує наявності нормативно-правової бази, формування концепції безпеки, розробку заходів, планів і процедур щодо безпечної роботи, проектування, реалізації та супроводу технічних засобів захисту інформації (ЗЗІ) в рамках освітньої установи. Ці складові визначають єдину політику забезпечення інформаційної безпеки у вищому навчальному закладі.

Метою статті є розгляд загально-концептуальних питань побудови і впровадження комплексної системи захисту (КСЗІ) інформаційних ресурсів ВНЗ України з урахуванням: виробничих і бізнес процесів, напрямів інформатизації та інформаційних активів, основних вимог до взаємодії підрозділів, складових інфраструктури та загально-технічних вимог до інформаційної системи, інформаційних технологій освітнього процесу, тощо.

Також, до сфери досліджень авторського колективу входить визначення основних проблем, що пов'язані з стандартизацією побудови КСЗІ інформації вищого навчального закладу; розробка загальних вимог для створення стандарту з урахуванням міжнародних та державних стандартів України; визначення науково обґрунтованих напрямів розробки стандарту.

Загальний аналіз міжнародних стандартів та вимог

З огляду на вищезазначене при формуванні системи інформаційної безпеки доцільно звернутися до міжнародного досвіду в галузі захисту інформації та бізнес процесів. Одними з найбільш важливих нормативно-технічних документів, які стимулюють розвиток захищених інформаційних систем, мереж і засобів є документи, що стандартизують вимоги та критерії оцінки безпеки.

Стандарт інформаційної безпеки*— це нормативно-правовий документ з забезпечення захисту інформації, який призначений для взаємодії між виробниками, споживачами і експертами у процесі створення та експлуатації захищених систем оброблення та передачі даних.*

Стандарти забезпечення захистузвичайно містять опис послідовності оцінок, які необхідно виконати, щоб вважати дану характеристику безпеки підтвердженою з точки зору атестації захисту або множину характеристик безпеки, які повинні забезпечити система захисту, щоб її можна було використовувати в даному конкретному режимі забезпечення безпеки або у відповідності до загальної стратегії захисту.

Найбільш практичними та ефективними стандартами інформаційної безпеки є (у хронологічному порядку): Критерії безпеки комп'ютерних систем, Європейські критерії безпеки інформаційних технологій, Федеральні критерії безпеки інформаційних технологій, Канадські критерії безпеки комп'ютерних систем, Загальні критерії безпеки інформаційних технологій та сімейство стандартів ISO.

Найбільш актуальними в сфері захисту інформації є сімейство стандартів ISO 27000 та безпосередньо основоположні:

- *ISO/IEC 27001:2005* «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги»;
- *ISO/IEC 27002:*2005 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою (раніше ISO/IEC 17799:2005)»;
- *ISO/IEC 27005:2008* «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки», тощо.

Стандарти сімейства ISO 27000 — це модель системи менеджменту, яка визначає загальну організацію, класифікацію даних, системи доступу, напрямки планування, методи забезпечення безпеки, практичні правила та вимоги, відповідальність співробітників, використання оцінки ризику і та ін. в контексті інформаційної безпеки підприємств. У процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої скорочення матеріальних втрат, зв'язаних з порушенням інформаційної безпеки.

Спеціальне законодавство у сфері безпеки інформаційної діяльності представлене сукупністю законів. У їх складі особливе місце належить базовим законам, які закладають основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

- інформації та інформаційних систем;
- суб'єктів — учасників інформаційних процесів;
- правовідносин виробників — споживачів інформаційної продукції;
- власників інформації — обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

Також слід приділити особливу увагу законам, що визначають засади захисту інформації в системах обробки і при її використанні з урахуванням категорій доступу до відкритої інформації та до інформації з обмеженим доступом. Важливу роль в інформаційній безпеці відіграють загальні норми з організації та підтримки інформаційних систем, включаючи банки даних державного призначення, порядку державної реєстрації, ліцензування, сертифікації, експертизи, а також загальні принципи захисту і гарантій прав учасників інформаційного процесу.

Таким чином, правовий захист інформації та стандартизація повинні забезпечуватися нормативно-законодавчими документами і актами, які являли б собою ієрархічну систему — від Конституції України до функціональних обов'язків і контракту окремого конкретного виконавця, що визначають перелік відомостей, що підлягають захисту, а також відповідальність за їх розголошення.

Аналіз існуючих проблем стандартизації побудови КСЗІ ВНЗ та шляхів їх вирішення

Слід зазначити, що ВНЗ в першу чергу є соціальним інститутом, призначення якого — виховання та професійна підготовка фахівців для різних сфер життєдіяльності суспільства. Від якості та безперервності підготовки залежить рівень розвитку економіки та суспільства в цілому.

Українська вища школа перебуває у процесі інформатизації, який має свої недоліки, що тісно пов’язані з активним впровадженням Інтернету та новітніх інформаційних технологій в навчальний процес. Одним із пріоритетних напрямів інформатизації ВНЗ є побудова комплексної системи захисту інформації.

Комплексна система захисту інформації ВНЗ — повинна бути системою збереження, обмеження та авторизованого доступу до інформації, що міститься на серверах в корпоративних мережах вузів, а також передана по інформаційно-комунікаційних каналах зв'язку в системах дистанційного навчання, тощо.

У більш широкому сенсі термін «комплексна система захисту інформації ВНЗ» повинна включати в себе два аспекти: систему захисту інтелектуальної власності ВНЗ від зовнішніх і внутрішніх агресивних впливів, систему управління доступом та захисту інформаційного простору від загроз. Останнім часом, у зв'язку з неконтрольованим масовим розвитком Інтернету, останній аспект безпеки стає особливо актуальним.

Під терміном «інформаційний простір» розуміється інформація, що міститься на серверах в корпоративних мережах навчальних закладів, установ, бібліотек, на електронних носіях та в глобальній мережі Інтернет.

Проблеми комплексної системи захисту корпоративних мереж ВНЗ набагато ширші, різноманітніші та гостріші, ніж в інших системах. Перш за все необхідно виділити наступні проблеми:

- корпоративна мережа ВНЗ будується зазвичай на концепції «обмеженого фінансування» (обладнання, кадри, неліцензійне програмне забезпечення);
- корпоративні мережі не мають стратегічних цілей розвитку(це означає, що топологія мереж, їх технічне і програмне забезпечення розглядаються з позицій поточних завдань);
- в одній корпоративній мережі ВНЗ вирішуються дві основні задачі: забезпечення освітньої та науковій діяльності, вирішення завдання управління освітнім і науковим процесами(це означає, що одночасно в цій мережі працює декілька автоматизованих систем або підсистем у рамках однієї системи управління);
- корпоративні мережі різнорідні як за обладнанням, так і за програмним забезпеченням, у зв'язку з тим, що створювалися протягом тривалого часу для різних завдань;
- відсутність централізованого управління інформаційною безпекою;
- плани комплексної системи захисту інформації, як правило, або відсутні, або не відповідають сучасним вимогам.

Це пов'язано з різноманіттям міжнародних та державних стандартів у галузі захисту інформації, але при цьому відсутністю єдиного національного стандарту для ВНЗ, який би регламентував планування, впровадження, перевірку та управління (обов’язково включаючи коригування) комплексною системою захисту інформації.

Особливості ВНЗ як об'єкта інформатизації пов'язані також з багатопрофільним характером діяльності, великою кількістю форм і методів навчальної роботи, просторової розгалуженої інфраструктури (філії, представництва). Сюди ж можна віднести і необхідність швидко адаптуватися до мінливого ринку освітніх та наукових послуг. Дещо полегшує проблему той момент, що ВНЗ є стабільною, ієрархічною за функціями управління системою, що володіє всіма необхідними умовами життєдіяльності і діє на принципах централізованого управління (останнє означає, що в управлінні завданнями інформатизації може активно використовуватися адміністративний ресурс).

Зазначені вище особливості обумовлюють необхідність дотримання наступних вимог при розробці узагальненого стандарту побудови комплексної системи захисту інформації вищого навчального закладу:

- комплексне опрацювання завдань інформаційної безпеки, починаючи з концепції і закінчуючи супроводом програмно-технічних рішень;
- залучення великої кількості фахівців, що володіють змістовною частиною ділових процесів;

• використання модульної структури корпоративних додатків, коли кожен модуль покриває взаємозв'язану групу ділових процедур або інформаційних сервісів при забезпеченні єдиних вимог до безпеки;

• застосування обґрунтованої послідовності етапів у вирішенні завдань інформаційної безпеки;

• документування розробок на базі розумного застосування стандартів, що гарантує створення ефективної системи;

• використання надійних і масштабованих апаратно-програмних платформ і технологій різного призначення, що забезпечують необхідний рівень безпеки.

З точки зору архітектури, в корпоративному інформаційному середовищі ВНЗ можна виділити три рівні, для забезпечення безпечного функціонування яких необхідно застосовувати різні підходи:

• обладнання обчислювальної мережі, каналів і ліній передачі даних, робочих місць користувачів, системи зберігання даних;

• операційні системи, мережеві служби і сервіси з управління обмеженням доступу до інформаційних ресурсів та об’єктів, програмне забезпечення середнього шару;

• прикладне програмне забезпечення, інформаційні сервіси і середовища (інформаційно-довідкові системи, бази даних та знань), орієнтовані на кінцевих користувачів.

При створенні комплексної системи захисту інформації необхідно забезпечити міжрівневе узгодження вимог з безпеки до вибору рішень або технологій, першочергово визначивши структурно-логічну структуру взаємодії підрозділів вищого навчального закладу, яка б включала в себе процедури обміну інформаційними потоками.

Для розробки ефективного спеціалізованого стандарту слід використати досвід зарубіжних країн (положення міжнародних стандартів), національний досвід (державні стандарти України) та звернути особливу увагу на особливості нормативно-правових документів, які використовуються у вищому навчальному закладі. Саме такий методологічний підхід дозволить досягти найкращого результату.

Висновки

В роботі досліджено загально-концептуальні питання побудови і впровадження КСЗІ інформаційних ресурсів ВНЗ України, а також розглянуто та визначено основні проблеми, що пов’язані з стандартизацією побудови КСЗІ інформації вищого навчального закладу з урахуванням міжнародних та державних стандартів. Визначено та обґрунтовано основні напрями розробки стандарту.

Список літератури

1. Віткін Л.М. Місце України у світовій та європейській якості. Стандартизація, сертифікація, якість — №3(18), 2002, с.43-49.

2. Зверард Кеменейд, Пол Гарр. Что требует бизнес и что дает вуз. Стандарты и качество, №10, 2001, с. 30-33.

3. Владимир Жуков.Управление качеством в системе непрерывного педагогического образования. Стандарты и качество, №9, 2002, с. 74-77

4. Юдін О.К. Матвійчук-Юдіна О.В.Яковенко О.Л. Методи розробки та впровадження комплексної інформаційно-довідкової системи підтримки навчального процесу. Збірка наукових праць інституту проблем моделювання в енергетиці .-К.:ІПМЕ НАН України, 2007 – спец.вип.. т.2 С. 123-124.