УДК 37.075

Г. Кононенко

annuta30@gmail.com

Київський національний університет технологій та дизайну, Київ

ПРОБЛЕМИ ІНФОРМАЦІЇНОЇ БЕЗПЕКИ ВИЩОЇ ОСВІТИ В УМОВАХ ГЛОБАЛІЗАЦІЇ

В умовах глобалізації та розвитку IT-технологій захищеність інформаційних ресурсів є однією з найважливіших складових успішного розвитку суспільства. На даному етапі розвитку відбувається впровадження сучасних інформаційних технологій, що суттєво впливає на зміни у процесах управління. Але відповідно до зростання кількості та складності інформації збільшується і кількість загроз інформаційної системи загалом. Заклади вищої освіти зіграли ключову роль у розвитку комп'ютерної техніки і програмного забезпечення. Вони розробляють, випробовують і впроваджують передові проекти в сфері IT. Зростання кіберзлочинності знижує захист конфіденційної інформації та розробок в навчальних закладах. Тому найбільш пріоритетним завданням в даний час є забезпечення інформаційної безпеки, успішне вирішення якого дозволить викладачам та студентам взаємодіяти один з одним, не турбуючись про збереження інформації.

В той же час сучасні технології, які забезпечують інформаційну безпеку допомагають навчальним закладам вирішувати різні типи завдань, наприклад організація захищеного доступу до освітніх матеріалів і систем з будь-якої точки світу.

При побудові системи інформаційної безпеки закладам вищої освіти необхідно враховувати ряд особливостей. У сучасному вузі зберігається і обробляється величезна кількість різних даних, пов'язаних 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.

Одна зі специфічних ознак захисту інформації в освітній системі полягає в тому, що вуз - публічний заклад з непостійною аудиторією, яка під впливом необмеженого використання та інших непередбачуваних факторів несе загрозу інформаційній безпеці мережі закладів вищої освіти.

Особливо гостро ставиться проблема інформаційної безпеки у сфері освіти у зв'язку з її інформатизацією. Все більше з'являється в мережі Інтернет різних освітніх ресурсів. На відміну від друкованої навчально-методичної літератури, яка проходить експертизу, в Інтернеті навчальний матеріал може розмістити будь-який бажаючий. Експертиза інформаційних освітніх ресурсів неможлива. Адже величезний обсяг інформації та комерційні умови доступу не завжди дозволяють оцінити якість таких ресурсів, грамотність, наукову достовірність [1].

Проблеми інформаційної безпеки мереж закладів вищої освіти набагато ширші, різноманітніші і гостріші, ніж в інших системах. Це пов'язано з такими особливостями:

- корпоративна мережа закладу вищої освіти будується, як правило, на основі мізерного фінансування (обладнання, кадри, неліцензійне програмне забезпечення);
- зазвичай корпоративні мережі не мають стратегічних цілей розвитку, а саме топологія мереж, їх технічне та програмне забезпечення розглядаються з позицій поточних завдань;
- в одній корпоративній мережі закладу вищої освіти вирішуються дві основні задачі: забезпечення освітньої та наукової діяльності і вирішення завдання управління освітнім та науковим процесами, тому одночасно в цій мережі працює кілька автоматизованих систем або підсистем в рамках однієї системи управління;
- корпоративні мережі гетерогенні як за обладнанням, так і за програмним забезпеченням у зв'язку з тим, що створювалися протягом тривалого періоду часу для різних завдань;
- плани інформаційної безпеки, як правило, або відсутні, або не відповідають сучасним вимогам.

У закладі вищої освіти можлива низка як внутрішніх, так і зовнішніх загроз безпеки інформації:

– спроби несанкціонованого адміністрування баз даних;

– дослідження мереж, несанкціонований запуск програм з аудиту мереж;

– видалення інформації, у тому числі бібліотек;

– запуск на виконання ігрових програм;

– установка вірусних програм і троянських коней;

– сканування мереж, у тому числі інших організацій через Інтернет;

– несанкціоноване скачування з Інтернету неліцензійного програмного забезпечення та інсталяція його на робочі станції;

– пошук “дірок” у операційній системі, міжмережевих екранах;

– спроби несанкціонованого віддаленого адміністрування операційних систем;

– сканування портів тощо[2].

У загальному вигляді і відповідно до міжнародних стандартів управління ризиками ІБ навчального закладу передбачає:

- визначення основних цілей і завдань захисту інформаційних активів закладів;
- створення ефективної системи оцінки та управління ризиками ІБ;
- розрахунок сукупності деталізованих якісно, а при можливості і кількісно оцінок ризиків;
- застосування спеціального інструментарію оцінки та управління ризиками із використанням для моделювання причинних взаємозв'язків, виявлених між концептами деякої області інформаційних і технічних аспектів закладів вищої освіти [3].

Проаналізувавши загрози інформаційної безпеки закладів вищої освіти можна запропонувати систему захисту, яка включає в себе чотири етапи:

1 етап – визначення та аналіз загроз інформаційної безпеки закладів вищої освіти;

2 етап – розроблення системи захисту інформації в вузі;

3 етап – реалізація плану захисту інформації;

4 етап – керування та контроль за функціонуванням системи захисту інформації.

На першому етапі побудови системи захисту інформації закладів вищої освіти необхідно здійснити аналіз об'єктивного захисту, ситуаційного плану, умов функціонування, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати дані для побудови окремої моделі загроз.

Джерелами загроз може бути витік інформації, порушення цілісності інформації, блокування інформації

На другому етапі побудови системи захисту інформації варто скласти план захисту інформації, який буде включати в себе наступні складові:

1. Розробка правового забезпечення захисту інформації. З одного боку, визначаються правила забезпечення інформаційної безпеки у закладі вищої освіти (наприклад, обов'язки співробітників), а з іншого - встановлюється відповідальність за їх порушення.

2. Складання переліку даних, що підлягають захисту. Інформація, яка використовується в вузах, може бути відкритою (доступна для всіх) або закритою (доступна для обмеженого кола осіб).

3. Створення підрозділу, відповідального за питання захисту інформації. У закладах вищої освіти всі питання пов'язані із застосуванням будь-яких програмних і апаратних засобів, включаються до компетенції ІТ-підрозділу.

4. Визначення основних напрямків забезпечення інформаційної безпеки. Основним питанням в плані забезпечення інформаційної безпеки є захист автоматизованої системи управління, яка здійснюється за рахунок застосування програмних і технічних засобів. Складність вирішення цього завдання обумовлюється двома факторами. По-перше, доступ до ресурсів системи має величезна кількість користувачів, які знаходяться у декількох розподілених підрозділах. По-друге, її робота будується на взаємодії цілого ряду програмних і апаратних компонентів.

На третьому етапі побудови системи захисту інформації необхідно реалізувати організаційні, первинні технічні й основні технічні заходи захисту інформації з обмеженим доступом, встановити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

Атестацію та сервісне обслуговування технічних засобів забезпечення інформації можуть здійснюватиюридичні й фізичні особи, які мають ліцензію на право проведення цих робіт, видану уповноваженим Кабінетом Міністрів України органом.

На четвертому етапі побудови системи захисту інформації варто провести аналіз функціонування системи захисту інформації, перевірку виконання заходів технічного захисту інформації, контроль ефективності захисту, підготувати й видати дані для керування системою захисту інформацією.

Керування системою захисту інформації полягає в адаптації заходів до поточного захисту [4].

Проведений аналіз уразливості інформаційних ресурсів Вищих навчальних закладів доцільно враховувати, що захист інформації потрібно здійснювати із застосуванням єдиної сукупності законодавчих, організаційних і технічних заходів, спрямованих на виявлення, відображення і ліквідацію різних видів загроз інформаційній безпеці. Оскільки система вищої освіти країни є вагомою складовою державної структури загалом та складною соціально-економічною системою, тому слід враховувати внутрішні та зовнішні чинники, що безпосередньо та опосередковано впливають на інформаційну безпеку цього закладу.

Література

1. Н. М. Кириленко, «Проблеми інформаційної безпеки освітнього середовища вищого навчального закладу», *Інформаційно-телекомунікаційні технології в сучасній освіті: досвід, проблеми, перспективи*: третя міжнар. наук.-практ. конф., ч.1, Львів, 2012, с. 149-151.

2. Н. П. Кухарська, «Оцінка інформаційного середовища вищих навчальних закладів та аналіз загроз його безпеці". *Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи»*, в. 4, ч. 2, с. 31–35, 2015.

3. О.О. Ільїн, «Когнітивна модель управління інформаційною безпекою вищого навчального закладу», *Науково-технічний журнал "Сучасний захист інформації"*, №2(30), с. 24–30,2017.

4. А. Нашинець-Наумова, «Організація системи захисту інформації суб'єктів господарювання», *Підприємство, господарювання і право*, № 2, с.110-116, 2016.

5. О. М. Проталинский, И. М. Ажмухамедов, «Информационная безопасность вуза», *Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ.*, № 1, 18–23, 2009.