УДК 004.056:378.1

Кухарська Н.П., канд. фіз.-мат. наук, доцент, Лагун А.Е., канд. техн. наук, доцент

Львівський державний університет безпеки життєдіяльності, м.Львів

ОЦІНКА ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ ТА АНАЛІЗ ЗАГРОЗ ЙОГО БЕЗПЕЦІ

Обґрунтовано необхідність розробки та впровадження збалансованої політики інформаційної безпеки вищих навчальних закладів. Розглянуто специфіку вузу як об’єкта інформації, яку необхідно враховувати при створенні комплексної системи інформаційної безпеки. В архітектурі інформаційного середовища освітнього закладу виокремлено основні об’єкти, що потребують захисту. Акцентовано увагу на особливостях побудови корпоративної мережі освітніх установ. Сформовано перелік можливих загроз інформаційної безпеки вищих навчальних закладів.

Ключові слова: вищий навчальний заклад, інформаційна безпека, загроза, інформація.

Обоснована необходимость разработки и внедрения сбалансированной политики информационной безопасности высших учебных заведений. Рассмотрена специфика вуза как объекта информации, которую необходимо учитывать при создании комплексной системы информационной безопасности. В архитектуре информационной среды образовательного учреждения выделены основные объекты, требующие защиты. Акцентировано внимание на особенностях построения корпоративной сети образовательных учреждений. Сформирован перечень возможных угроз информационной безопасности высших учебных заведений.

Ключевые слова: высшее учебное заведение, информационная безопасность, угроза, информация.

In this paper is proved necessity of balanced development and implementation of information security policy in higher education. Also is showed the specificity of the university as an object of information that should be considered when establishing a comprehensive information security system. In the architecture of the information environment of educational institutions singled out the main items that need protection. The attention is focused on the features of corporate network of educational institutions. And also is Formed a list of possible threats to information security universities.

Keywords: university, information security, threat, information.

У Доктрині інформаційної безпеки України зазначено: “Інформаційна безпека (ІБ) є невід'ємною складовою кожної зі сфер національної безпеки”. В умовах стрімкого розвитку науково-технічних засад інформаційного суспільства одним із пріоритетних напрямків державної політики у галузі інформаційної

безпеки є вдосконалення системи підготовки фахівців відповідних кваліфікацій, розвиток освіти у цій сфері. Ключова роль у вирішенні поставлених завдань відводиться вищому навчальному закладу (ВНЗ). Разом з тим, вітчизняна вища школа перебуває зараз на етапі адаптації як до об'єктивних процесів інформаційного суспільства, так і до нових соціально-політичних умов з характерними для них проявами конкурентної боротьби.

Зростання кількості злочинів у сфері інформаційних технологій диктує свої вимоги до захисту інформаційних ресурсів навчальних закладів і ставить завдання побудови власної інтегрованої системи безпеки. Його вирішення передбачає наявність нормативно-правової бази, формування концепції безпеки, розробку заходів, планів, процедур щодо безпечної роботи, проектування, реалізацію і супровід технічних та інших засобів захисту інформації освітньої установи.

Створення ефективних механізмів управління інформаційними ресурсами системи вищої освіти в сучасних умовах неможливе без наукового обґрунтування та практичної реалізації збалансованої політики інформаційної безпеки вузу, в тому числі процедури визначення загроз ІБ ВНЗ.

Мета статті – проаналізувати специфіку інформаційного середовища ВНЗ та сформувати перелік можливих загроз безпеці його інформаційних активів.

Особливості ВУЗу як об'єкта інформатизації пов'язані з багатопрофільним характером діяльності, великою кількістю форм і методів навчальної роботи, просторовим рознесенням 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 вищими органами, часта зміна статусу працівників та студентів [1].

У сучасному вузі зберігаються і обробляються у великому обсязі різні дані, пов'язані не тільки із забезпеченням навчального процесу, але і з науково-дослідними та проектно-конструкторськими розробками, персональні дані студентів і працівників, службова, комерційна та інша конфіденційна інформація.

Звернемо увагу ще на одну специфіку вузу, яку слід враховувати при створенні та впровадженні комплексної систему захисту інформації. ВНЗ – це публічна установа з аудиторією, що постійно змінюється. Крім того, вищий навчальний заклад є місцем підвищеної концентрації початківців-хакерів, які, як відомо, не цураються будь-якої нагоди продемонструвати свій хист. До основної групи потенційних порушників у вузах належать студенти. Багато з них мають доволі високий рівень підготовки у сфері інформаційних технологій. Вік (від 17 до 22 років) і юнацький максималізм спонукає деяких молодих людей похизуватися своїми знаннями та вміннями перед однокурсниками: влаштувати вірусну епідемію, отримати адміністративний доступ і нашкодити викладачеві, заблокувати вихід в Інтернет і т.д.

При цьому трохи полегшує вирішення проблеми забезпечення інформаційної безпеки той факт, що ВНЗ є стабільною, ієрархічною за функціями управління системою, що володіє всіма необхідними умовами життєдіяльності, діючою на принципах централізованого управління (а це означає, що в управлінні завданнями інформатизації може активно використовуватися адміністративний ресурс).

З точки зору архітектури, в корпоративному інформаційному середовищі можна виокремити 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 доступом до інформаційних ресурсів;

- прикладне програмне забезпечення, інформаційні сервіси та середовища, орієнтовані на користувачів.

Проблеми комплексної інформаційної безпеки корпоративних мереж ВНЗ набагато ширші, різноманітніші і гостріші, ніж в інших системах. Це пов'язано з такими особливостями:

- корпоративна мережа ВНЗ 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 ВНЗ 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 (автоматизована система управління (АСУ) “Студент”, АСУ “Кадри”, АСУ “Навчальний процес”, АСУ “Бібліотека”, АСУ “НДР” АСУ “Бухгалтерія” і т.д.);
- 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 комплексної інформаційної безпеки, як правило, або відсутні, або не відповідають сучасним вимогам.

У такій мережі 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;
- спроби злому АСУ “ВНЗ”;
- сканування мереж, у тому числі інших організацій через Інтернет;
- несанкціоноване скачування з Інтернету неліцензійного програмного забезпечення та інсталяція його на робочі станції;
- спроби проникнення в системи бухгалтерського обліку;
- пошук “дірок” у операційній системі, міжмережевих екранах, Proxy-серверах;
- спроби несанкціонованого віддаленого адміністрування операційних систем;
- сканування портів тощо.

Основними об'єктами ВУЗу, що потребують захисту, є:

- бухгалтерські локальні обчислювальні мережі, дані планово-фінансового відділу, а також статистичні та архівні дані;
- сервери баз даних;
- консоль управління обліковими записами;
- www/ftp сервери;
- локальні обчислювальні мережі і сервери дослідницьких проектів.

Визначимо ненавмисні та навмисні суб’єктивні, техногенні та природні загрози інформаційних активів ВНЗ.

Ненавмисні суб’єктивні загрози ІБ ВНЗ:

- загроза ненавмисного пошкодження обладнання;
- загроза неправомірного відключення устаткування;
- загроза ненавмисного видалення файлів з важливою інформацією;
- загроза ненавмисного спотворення файлів з важливою інформацією;
- загроза ненавмисного видалення програм;
- загроза ненавмисного внесення змін до програми;
- загроза неправомірної зміни режимів роботи пристроїв;

- загроза ненавмисної псування носіїв інформації;
- загроза некомпетентного запуску технологічних програм;
- загроза використання нелегального програмного забезпечення;
- загроза зараження комп'ютера вірусами;
- загроза необережних дій, що призводять до порушення конфіденційності;
- загроза розголошення, передачі або втрати атрибутів розмежування доступу;
- загроза ігнорування організаційних обмежень при роботі з інформаційними ресурсами;
- загроза входу в систему в обхід засобів захисту;
- загроза вчинення ненавмисної помилки при проектуванні та обслуговуванні інформаційної системи (ІС);
- загроза некомпетентного використання і налаштування засобів захисту інформації (ЗІ);
- загроза неправомірного відключення засобів ЗІ персоналом служби безпеки;
- загроза пересилання даних за помилковим адресом абонента;
- загроза введення помилкових даних.

Навмисні суб'єктивні загрози ІБ ВНЗ:

- загроза навмисного фізичного руйнування системи;
- загроза виведення з ладу найбільш важливих компонентів ІС;
- загроза відключення підсистем забезпечення ІС;
- загроза виведення з ладу підсистем забезпечення ІС;
- загроза навмисного порушення режимів експлуатації пристроїв або режимів використання програмного забезпечення;
- загроза саботажу з боку персоналу;
- загроза впровадження агентів в персонал ІС;
- загроза вербування персоналу;
- загроза застосування технічних засобів розвідки;

- загроза перехоплення побічного електромагнітного випромінювання та наведень;
- загроза перехоплення інформації в каналах зв'язку та її аналізу;
- загроза здійснення “маскараду”;
- загроза розкрадання носіїв інформації;
- загроза несанкціонованого копіювання інформації;
- загроза розкрадання виробничих відходів;
- загроза читання залишкової інформації з оперативних та зовнішніх запам'ятовуючих пристроїв;
- загроза незаконного отримання реквізитів розмежування доступу;
- загроза злому шифрів криптографічного захисту інформації;
- загроза застосування апаратних закладок;
- загроза застосування програмних закладок і вірусів.
- загроза роботи “між рядками”;
- загроза фальсифікації даних;
- загроза модифікації потоку даних.

Техногенні загрози:

- загроза збою технічних засобів обробки інформації (ТЗОІ);
- загроза відмови ТЗОІ;
- загроза збою допоміжних технічних засобів;
- загроза відмови допоміжних технічних засобів;
- загроза збою системи електропостачання;
- загроза збою системи клімат-контролю;
- загроза збою зовнішніх інформаційних каналів комунікації;
- загроза відмови зовнішніх інформаційних каналів комунікації;
- загроза відмови систем водопостачання і каналізації на об'єкті інформатизації (ОІ);

- загроза помилкового спрацьовування систем пожежогасіння на ОІ;
- загроза помилкового спрацьовування охоронної сигналізації на ОІ;

Стихійні загрози:

- загроза пожежі;
- загроза повені;
- загроза землетрусу;
- загроза ураження блискавкою;
- загроза урагану;
- загроза екстремально високої температури на ОІ;
- загроза екстремально низької температури на ОІ.

Кожна з перерахованих загроз має апріорну ймовірність виникнення, залежну від привабливості інформаційного активу для зловмисника, рівня його кваліфікації, стану зовнішньої інфраструктури, кліматичних умов, місця розташування об'єкту. Від повноти та всебічності проведеного аналізу загроз інформаційної безпеки залежить ефективність розробки та впровадження у вищому навчальному закладі комплексної системи захисту інформації.

Література

1. Ажмухамедов И. М. Информационная безопасность ВУЗа / Ажмухамедов И.М. // Инновационная деятельность в сфере образования и науки – приоритетное направление политики государства : Материалы 1 международной заочной научно-практической конференции. – Астрахань, 2009. – С. 133-139.