УДК 004.056:378.147

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ОДИН ІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

З.П. Сташевський, ад'юнкт; Н.Є. Бурак, викладач;
Ю.І. Грицюк д-р техн. наук, проф. – Львівський ДУ БЖД

Інформація – текстова, числова, графічна, звукова, незалежно від того, чи є вона власністю держави, суспільства або окремих організацій чи фізичних осіб, становить певну цінність. Тому інформаційний ресурс потребує постійного захисту від різних сторонніх впливів і джерел загроз, які можуть призвести до зниження їхньої цінності, порушення конфіденційності, цілісності та доступності. Розвиток інформаційних систем, їх ускладнення, взаємна інтеграція та відкритість призводять до появи нових джерел загроз інформації, зростання кількості зловмисників, котрі мають потенційну можливість здійснити вплив на неї.

Для успішної роботи сучасних інформаційних систем потрібні фахівці з інформаційної безпеки, які вміло коригуватимуть роботу програмного та технічного забезпечення. У Львівському державному університеті безпеки життєдіяльності (ЛДУ БЖД) значне місце у підготовці фахівців даної галузі знань [3] покладено на систему дистанційного навчання "Віртуальний університет", яку створено на базі середовища Moodle. Умовою забезпечення надійного захисту інформації у цій системі є розроблення та впровадження політики інформаційної безпеки. За її відсутності у аналогічній системі можуть виникати протиправні дії зловмисників щодо курсів навчальних програм загалом, так і кожного з користувачів (викладач, курсант/студент, ад'юнкт) зокрема [1].

Підготовка фахівців з інформаційної безпеки для потреб структурних підрозділів МНС України, в силу специфіки виконуваних робіт і вирішуваних завдань, вимагає ознайомлення та вивчення методологій побудови системи захисту інформації, спрямованої на захист конфіденційних даних потенційно небезпечних об'єктів, об'єктів підвищеної небезпеки, хімічно небезпечних об'єктів та інших важливих державних установ, що містять або можуть містити державну таємницю. В зв'язку з цим у ЛДУ БЖД дистанційний доступ до лекційних матеріалів і навчальних програм у системі дистанційного навчання "Віртуальний університет" є дещо обмеженим. Регулювання доступом до інформаційних ресурсів здійснюється на основі вибору тої чи іншої політики безпеки.

Під *політикою безпеки* розумітимемо набір норм, правил і практичних прийомів, які регулюють процес управління цінною інформацією, її захист і розподіл. Вона забезпечує: захист інформаційних активів організації; безперебійну та стабільну діяльність організації; мінімум ризиків інформаційної безпеки; створення позитивних інформаційних відносин організації з партнерами, клієнтами та всередині неї.

Основним завданням політики безпеки у системі дистанційного навчання "Віртуальний університет" є захист інформаційних активів від зовнішніх і внутрішніх навмисних і ненавмисних джерел загроз. Наявність політики безпеки наявних інформаційних ресурсів та її формального опису у вигляді відповідної моделі за умови дотримання інформаційною системою встановлених правил та обмежень дає змогу перевірити її відповідність визначеному критерію ефективності.

Поняття політики безпеки інформаційних ресурсів порівняно із поняттям несанкціонованого доступу до інформації є ширшим. Політика безпеки оперує поняттями дозволених і не дозволених доступів до інформаційних ресурсів. Виконання політики безпеки у системі дистанційного навчання "Віртуальний університет" забезпечує необхідні, а інколи і достатні умови безпеки самої інформаційної системи.

У сучасній теорії захисту інформації [2] розглядають такі політики безпеки інформаційних ресурсів: дискретна (розмежувальна); мандатна (багаторівнева); ролевого розмежування доступів; ізольованого програмного середовища; безпеки інформаційних потоків та ін.

Дискретна політика безпеки (за іншими перекладами – розмежувальна) базується на дискретному управлінні доступом до інформаційних ресурсів. Вона передбачає, що права доступу суб'єктів до кожного окремого об'єкта інформаційної системи можуть бути довільно обмежені на основі деякого зовнішнього правила доступу до системи. Також ця політика вимагає ідентифікованості всіх суб'єктів і об'єктів інформаційної системи.

Недоліком цієї політики є статичність правил розмежування доступу до ресурсів, які не враховують динаміки зміни стану інформаційної системи. Також під час доступу суб'єкта до об'єкта інформаційної системи щоразу слід визначати права доступу до інформаційних ресурсів і аналізувати їхній вплив на безпеку системи загалом, що робить її менш прозорою.

Мандатна політика безпеки (за іншими перекладами – нормативна, примусова, або багаторівнева) базується на мандатному управлінні доступом до інформаційних ресурсів. Ця політика передбачає виконання таких умов: визначеність решітки конфіденційності інформації; надання кожному об'єкту системи певного рівня конфіденційності, який визначає цінність інформації, що міститься в цьому об'єкті; задоволення вимог ідентифікованості всіх суб'єктів та об'єктів системи. Головне завдання мандатної політики безпеки полягає у запобіганні витоку інформації від об'єктів, що мають високий рівень доступу, до об'єктів із низьким рівнем доступу.

На сьогодні найпоширенішим описом мандатної політики безпеки є модель Белла-ЛаПадула[1]. Основним недоліком мандатної політики безпеки є високі вимоги до обчислювальних ресурсів і складність практичної реалізації такої системи.

---

[1]Модель Белла-ЛаПадула – модель контролю та управління доступом до інформаційних ресурсів, яка базується на мандатній моделі, проте у ній аналізуються умови, при яких неможливе створення інформаційних потоків від суб'єктів з більш високим рівнем доступу до суб'єктів з нижчим рівнем доступу.

Політика рольового розмежування доступу базується на дискретній політиці безпеки та є її удосконаленим варіантом. Згідно з цією політикою, права доступу суб'єктів інформаційної системи формуються згідно з їхніми повноваженнями й обов'язками (ролями). Ця політика відрізняється від інших політик своєю гнучкістю. Її активно використовують у мережевих операційних системах, великих системах управління базами даних, де встановлено чіткі повноваження й обов'язки адміністраторів і користувачів інформаційної системи. На основі цієї політики часто реалізують інші політики, зокрема й мандатну.

Політика ізольованого програмного середовища визначає безпечний порядок взаємодії суб'єктів інформаційної системи, який унеможливлює появу нових суб'єктів і їхній вплив на систему захисту інформації через небезпечну модифікацію чи конфігурацію її параметрів. Згідно з цією політикою, вся множина інформаційних потоків у інформаційній системі поділяється на дві підмножини, що не перетинаються, – потоки несанкціонованого доступу і потоки легального доступу. Потоки несанкціонованого доступу підлягають фільтрації. Такий розподіл інформаційних потоків і їх фільтрація має здійснюватися певним суб'єктом інформаційної системи, який отримав назву монітор безпеки об'єктів.

Політика безпеки інформаційних потоків визначає безпечний порядок взаємодії об'єктів інформаційної системи у самій системі. Ця політика полягає в розподілі множини інформаційних потоків у системі на дві підмножини, що не перетинаються, – бажаних і не бажаних, і унеможливлює появу в інформаційній системі не бажаних інформаційних потоків [2, ст. 66-68].

Система дистанційного навчання "Віртуальний університет" ЛДУ БЖД передбачає управління великими базами даних (індивідуальні дані користувачів, навчальні програми, лекційні та лабораторні матеріали, репозитарій тощо) та надання доступу до певної інформації різним категоріям користувачів (педагогічний склад, курсанти/студенти, ад'юнкти). Проведений вище огляд ряду найпоширеніших політик безпеки, які можуть застосовуватися до різних інформаційних систем, показав, що найоптимальнішою з них для даного навчального середовища є політика рольового розмежування доступу до інформаційних ресурсів, яка дає змогу покращити підготовку фахівців з захисту інформації для потреб структурних підрозділів МНС України.

1. Голубченко О.Л. Політика інформаційної безпеки / О.Л. Голубченко. – Луганськ : Вид-во СНК ім. В. Даля, 2009. – 300 с.

2. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / Грайворонський М.В., Новіков О.М. – К. : Вид. група BHV, 2009. – 608 с.

3. Грицюк Ю.І. Проблема підготовки фахівців з інформаційної безпеки структурних підрозділів Міністерства надзвичайних ситуацій України / Грицюк Ю.І., Рак Т.Є.// Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту : матер. Міжнар. наук. конф. [зб. наук. праць у 2-ох т.], 16-20 травня 2011 р., м. Євпаторія. – Херсон : Вид-во ХНТУ. – 2010. – Т. 2. – С. 272-276.