УДК 004.056:061.68

З. П. Сташевський, О. І. Лозинський, Н. Є. Бурак
(Львівський державний університет безпеки життєдіяльності)

ВПРОВАДЖЕННЯ ПОЛІТИКИ РОЛЬОВОГО РОЗМЕЖУВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ У СИСТЕМІ ДИСТАНЦІЙНОГО НАВЧАННЯ

Проведено аналіз моделей існуючих політик інформаційної безпеки як однієї з основних складових системи захисту інформації. На основі проведеного аналізу визначено найбільш оптимальну політику, основною функцією якої є захист інформаційних ресурсів (курси навчальних програм, особисті дані користувачів, репозитарій та ін.) системи дистанційного навчання "Віртуальний університет" Львівського державного університету безпеки життєдіяльності. Наведено модель рольового розмежування доступу до цієї навчальної системи, що дає змогу забезпечити належний рівень захисту інформації від зовнішніх і внутрішніх загроз.

Ключові слова: система дистанційного навчання, "Віртуальний університет", середовище Moodle, політика безпеки, інформаційний ресурс, джерела загроз.

Вступ. Інформаційні технології як невід'ємна складова сучасного суспільства все глибше проникають практично в усі сфери діяльності людини. Водночас людство все інтенсивніше їх використовує. Застосування інформаційних технологій має значні переваги: підвищується ефективність процесу управління; значно збільшується швидкість оброблення та передачі даних; покращується захист інформації від зловмисних дій і т.п. Саме тому забезпечення безпеки не тільки самої інформації, але й безпосередньо інформаційних технологій, є актуальною проблемою, яка потребує нагального вирішення.

Сьогодні важко уявити будь-який структурний підрозділ Державної служби України з надзвичайних ситуацій без застосування новітніх інформаційних технологій [4], починаючи від автоматизації окремих робочих місць оперативно-диспетчерської служби і закінчуючи побудовою корпоративних розподілених інформаційних мереж. Основною метою будь-якої системи захисту інформації в структурних підрозділах Державної служби України з надзвичайних ситуацій [9] є створення надійних умов її функціонування, запобігання та ліквідація джерел загроз, захист законних інтересів працівників від протиправних посягань зловмисників, недопущення розголошення, втрати, витоку, спотворення та знищення службової інформації. Однак, розвиток інформаційних систем, їх ускладнення, взаємна інтеграція та відкритість призводять до появи нових джерел загроз, зростання кількості зловмисників, котрі мають потенційну можливість здійснити вплив на неї [7].

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

Мета роботи: провести аналіз відомих політик інформаційної безпеки, які можуть використовуватися в системі дистанційного навчання "Віртуальний університет" ЛДУ БЖД, навести модель рольового розмежування доступу до інформаційних ресурсів цієї системи.

1. Характеристика політик безпеки сучасних інформаційних ресурсів

Підготовка фахівців з захисту інформації на сьогодні, в силу специфіки виконуваних робіт і вирішуваних завдань, вимагає ознайомлення та вивчення методологій побудови системи захисту інформації (СЗІ), 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 дистанційний доступ до лекційних матеріалів і навчальних програм у системі дистанційного навчання "Віртуальний університет" ЛДУ БЖД має бути обмеженим. Регулювання доступу до інформаційних ресурсів має здійснюватися 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 [8]. 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 є захист інформаційних активів від зовнішніх і внутрішніх навмисних і ненавмисних джерел загроз. Наявність політики безпеки сучасних 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. В нашому випадку це безпосередньо стосується системи дистанційного навчання "Віртуальний університет".

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 забезпечує необхідні, а інколи і достатні умови безпеки інформаційної системи.

У сучасній теорії захисту інформації розглядають такі політики безпеки інформаційних ресурсів: дискретна (розмежувальна); мандатна (багаторівнева); рольового розмежування доступів; ізольованого програмного середовища; безпеки інформаційних потоків та ін. Розглянемо кожну з них детальніше.

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 потребує ідентифікації всіх суб'єктів і об'єктів інформаційної системи.

Недоліком цієї політики є статичність правил розмежування доступу, 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. Для інформаційних систем з дискретною політикою безпеки задача перевірки безпеки є алгоритмічно нерозв'язною. Припущення, що система, в якій реалізовано дискреційну політику безпеки, є захищеною у заданому стані, слід доводити для кожної конкретної системи і для кожного її стану.

Мандатна політика безпеки (за іншими перекладами – нормативна, примусова або багаторівнева) базується на мандатному управлінні доступом до інформаційних ресурсів (рос. – мандатное, нормативное, полномочное, принудительное управление доступом, англ. – mandatory access control). 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] [5, ст. 61-65], згідно з якою суб'єкт зможе отримати доступ до інформації лише за умови, що матиме на це достатні повноваження, і будь-який суб'єкт (окрім адміністратора, якому надано повноваження встановлювати рівні конфіденційності об'єктів) у жодному разі не зможе здійснити перенесення даних із об'єкта з вищим рівнем конфіденційності в об'єкти нижчих ієрархічних рівнів. Отже, ця модель забезпечує конфіденційність доступу до інформаційних ресурсів, а інформаційні системи, побудовані на ній, є більш надійними, ніж системи, створені на основі дискретної політики безпеки.

Недоліками мандатної політики безпеки є високі вимоги до обчислювальних ресурсів і складність практичної реалізації такої системи.

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].

Отже, 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.

2. Модель рольового розмежування доступу до інформаційних ресурсів системи дистанційного навчання "Віртуальний університет"

Основними елементами моделі рольового розмежування доступу (РРД) до інформаційних ресурсів системи дистанційного навчання "Віртуальний університет" ЛДУ БЖД є:

- $\boldsymbol{U} = \{u_i, i = \overline{1,n}\}$ – множина користувачів системи: педагогічний склад, курсанти/студенти, ад'юнкти та ін.;
- $\boldsymbol{R} = \{r_i, i = \overline{1,n}\}$ – множина ролей системи: manager – адміністратор; course creator – автор курсу; teacher – викладач; non-editing teacher – викладач без права редагування;

[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.

student – курсанти/студенти; guest – відвідувач; authenticated user – авторизований користувач та ін.;

- $\boldsymbol{P} = \{p_i, i = \overline{1,m}\}$ – множина прав доступу до об'єктів системи: навчальні курси, науковий репозитарій, особисті дані користувачів та ін.;
- $\boldsymbol{S} = \{s_i, i = \overline{1,n}\}$ – множина сеансів роботи користувачів системи, статистика роботи користувачів;
- $PA: \boldsymbol{R} \to 2^{\boldsymbol{P}}$ – функція, яка визначає для кожної ролі системи множину прав доступу; при цьому для кожного $p \in \boldsymbol{P}$ існує $r \in \boldsymbol{R}$ така, що $p \in PA(r)$;
- $UA: \boldsymbol{U} \to 2^{\boldsymbol{R}}$ – функція, яка визначає для кожного користувача системи множину ролей, на які він може авторизуватися;
- $user: \boldsymbol{S} \to \boldsymbol{U}$ – функція, яка визначає для кожного сеансу відповідного користувача системи, від імені якого він активований;
- $roles: \boldsymbol{S} \to 2^{\boldsymbol{R}}$ – функція, яка визначає для користувача системи множину ролей, на які він авторизований в цьому сеансі; при цьому в кожен момент часу τ для кожного сеансу $s \in \boldsymbol{S}$ має виконуватися умова $roles(s) \subseteq UA(user(s))$. Принципово можуть існувати ролі системи, на які не авторизований жоден користувач.

У моделі РРД до інформаційних ресурсів передбачається, що множини ***U***, ***R***, ***P*** і функції ***PA***, ***UA*** не змінюються з часом. Множина ролей, на які авторизується користувач впродовж одного сеансу роботи, модифікується самим користувачем. У моделі РРД відсутні механізми, які дають змогу одному сеансу активізувати інший сеанс, тобто усі сеанси можуть активізуватися тільки користувачем.

Для забезпечення відповідності реальним інформаційним системам, кожен користувач, яких займає певне положення в службовій ієрархії системи дистанційного навчання "Віртуальний університет", на множині ролей реалізується ієрархічна структура доступу до інформаційних ресурсів.

Ієрархією ролей у моделі РРД називатимемо задане на множині ролей ***R*** відношення часткового порядку "≤", яке має властивості рефлексивності, антисиметричності та транзитивності. При цьому виконується умова для

$$u \in \boldsymbol{U}, \text{ якщо } r, r' \in \boldsymbol{R}, r \in UA(u) \text{ і } r' \le r, \text{ то } r' \in UA(u).$$

Це означає, що разом з цією роллю користувач має бути авторизований на усі ролі в її нижчих рівнях ієрархії.

Іншим важливим механізмом реалізації моделі РРД до інформаційних ресурсі системи дистанційного навчання "Віртуальний університет" є обмеження, що накладаються на множину ролей, на які може авторизуватися користувач або на які він авторизується впродовж одного сеансу. У моделі РРД можуть задаватися обмеження статичного взаємного виключення ролей або прав доступу, якщо виконуються такі умови:

$$\boldsymbol{R} = R_1 \cup ... \cup R_n, \text{ де } R_i \cap R_j = \varnothing \text{ для } 1 \le i \le j \le n;$$

$$\left|UA(u) \cap R_i\right| \le 1 \text{ для } u \in \boldsymbol{U}, \ i = \overline{1,n};$$

$$\boldsymbol{P} = P_1 \cup ... \cup R_m \text{ де } P_i \cap P_j = \varnothing \text{ для } 1 \le i \le j \le m;$$

$$\left|PA(r) \cap P_i\right| \le 1 \text{ для } p \in \boldsymbol{U}, \ i = \overline{1,m},$$

тобто, множина ролей і множина прав доступу розділяються на підмножини, що не перетинаються. При цьому кожен користувач може мати не більше однієї роллі з кожної підмножини ролей, а кожна роль – може мати не більше, ніж одне право доступу з кожної підмножини прав доступу.

У моделі РРД до інформаційних ресурсів можуть задаватися обмеження динамічного взаємного виключення ролей, якщо виконуються такі умови:

$$\boldsymbol{R} = R_1 \cup ... \cup R_n, \text{ де } R_i \cap R_j = \varnothing \text{ для } 1 \le i \le j \le n;$$

$$\left| roles(s) \cap R_i \right| \le 1 \text{ для } s \in \boldsymbol{S}, i = \overline{1,n},$$

тобто, множина ролей розділяється на підмножини, що не перетинаються. При цьому в кожному сеансі користувач може мати не більше, ніж одну ролль з кожної підмножини ролей.

У моделі РРД можуть задаватися статичні кількісні обмеження можливості мати ролль або право доступу, якщо визначено дві функції:

$$\alpha : \boldsymbol{R} \to \boldsymbol{N}_0; \qquad \beta : \boldsymbol{P} \to \boldsymbol{N}_0$$

та виконуються дві умови:

$$\left| UA^{-1}(r) \right| \le \alpha(r) \text{ для } r \in \boldsymbol{R};$$

$$\left| PA^{-1}(p) \right| \le \beta(p) \text{ для } p \in \boldsymbol{P},$$

де $\boldsymbol{N}_0$ – множина натуральних чисел з нулем. Тобто, для кожної ролі РРД у системі дистанційного навчання "Віртуальний університет" може встановлювать максимальна кількість користувачів, які будуть в ній авторизовані, а для кожного права доступу може встановлюватися максимальна кількість ролей, які будуть ними володіти.

У моделі РРД може задаватися динамічне кількісне обмеження на володіння роллю, якщо визначена функція:

$$\gamma : \boldsymbol{R} \to \boldsymbol{N}_0$$

і виконується така умова:

$$\left| roles^{-1}(r) \right| \le \gamma(r) \text{ для } r \in \boldsymbol{R},$$

тобто, для будь-якої ролі встановлюється максимальна кількість сеансів роботи користувачів, які можуть одночасно на них авторизуватися.

У моделі РРД у системі дистанційного навчання "Віртуальний університет" можуть задаватися статичні обмеження необхідного володіння роллю або правом доступу, якщо визначено дві функції:

$$\alpha : \boldsymbol{R} \to 2^{\boldsymbol{R}}; \qquad \beta : \boldsymbol{P} \to 2^{\boldsymbol{P}}$$

і виконуються такі умови:

- для $u \in \boldsymbol{U}$ якщо $r, r' \in \boldsymbol{R}, r \in UA(u)$ і $r' \in \alpha(r)$, то $r' \in UA(u)$;
- для $r \in \boldsymbol{R}$, якщо $p, p' \in \boldsymbol{R}, p \in PA(r)$ і $p' \in \beta(p)$, то $p' \in PA(r)$,

тобто, для кожної ролі для того, щоб в ній зміг авторизуватися користувач, можуть визначатися ролі, на які користувач також має авторизуватися.

У моделі РРД може задаватися динамічне обмеження необхідного володіння роллю, якщо визначена функція

$$\gamma : \boldsymbol{R} \to 2^{\boldsymbol{R}}$$

і виконується така умова:

для $s \in \boldsymbol{S}$, якщо $r \in \boldsymbol{R}, r \in roles(s)$ і $r' \in \gamma(r)$, то $r' \in roles(s)$,

тобто, для кожної ролі для того, щоб в ній зміг авторизоватися користувач в деякому сеансі роботи, можуть визначатися ролі, на які користувач також має авторизуватися в цьому сеансі [5, ст. 88-91].

Загальна схема моделі РРД до інформаційних ресурсів системи дистанційного навчання "Віртуальний університет" зображена на рис. 1.

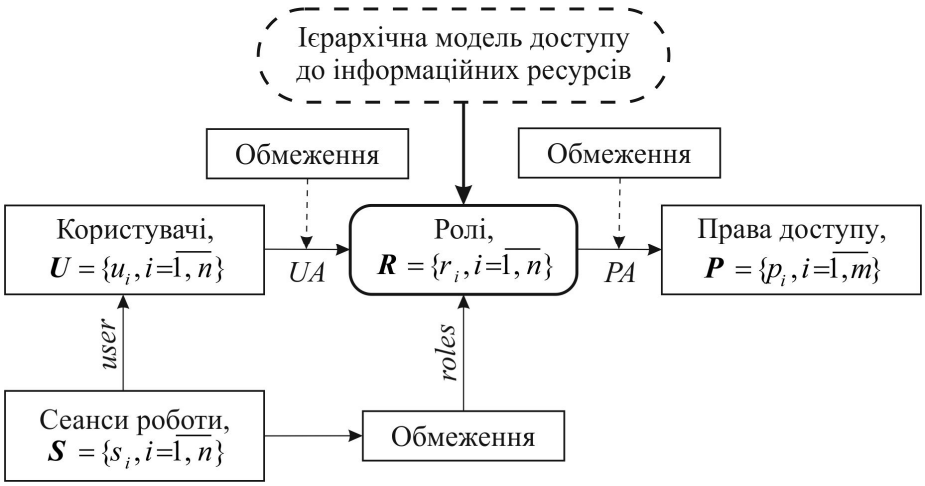

Рис. 1. *Схема моделі РРД до інформаційних ресурсів системи дистанційного навчання "Віртуальний університет"*

Рівні доступу, які використовуються у системі дистанційного навчання "Віртуальний університет":

- *Manager (адміністратор)* – має найвищий рівень доступу;
- *Course creator (автор курсу)* – може створювати курси та призначати викладачів у них;
- *Teacher (викладач)* – може робити будь-які зміни в своєму курсі;
- *Non-editing teacher (викладач без права редагування)* – не може робити змін у курсі, а лише ставити оцінки;
- *Student (курсанти/студенти)* – слухач курсу, який може виконувати завдання, проходити курс, тестуватися в ньому і т.д.;
- *Guest (відвідувач)* – має обмежений доступ, може лише переглядати деякі елементи курсу за наявності в ньому доступу для гостей;
- *Authenticated user* – усі авторизовані користувачі.

Призначенням прав кожного з користувачів системи дистанційного навчання "Віртуальний університет" займається адміністратор (manager), однак викладач у своєму курсі може призначити собі співвикладача [6].

Отже, модель рольового розмежування доступу дає змогу чітко встановити рівні доступу кожного користувача системи до тої чи іншої інформації, що міститься в навчальних програмах, репозитарії та ін., проводити статистику сеансів роботи користувача. Чітко встановлені рівні доступу до інформаційних ресурсів запобігають діям зловмисників, спрямованим на зміну властивостей інформації – цілісність, доступність, конфіденційність.

Висновки:

1. Проведено аналіз сучасних політик інформаційної безпеки для забезпечення захисту інформації у системі дистанційного навчання "Віртуальний університет" Львівського ДУБЖД.

2. Адаптовано модель рольового розмежування доступу до інформаційних ресурсів в систему дистанційного навчання "Віртуальний університет", що дає змогу забезпечити належний захист наявної там інформації від зовнішніх і внутрішніх джерел загроз.

Список літератури:

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.

4. Грицюк Ю.І. Проблеми захисту інформації у структурних підрозділах МНС України / Грицюк Ю.І., Рак Т.Є. // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2011. – Вип. 21.12. – С. 330-346.

5. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособ. [для студ. ВУЗ] / П.Н. Девянин. – М. : Изд. центр "Академия", 2005. – 144 с.

6. Козяр М.М. Віртуальний університет : навч.-метод. посібн. / М.М. Козяр, Т.Є. Рак, О.Б. Зачко. – Львів : Вид-во ЛДУ БЖД, 2009. – 168 с.

7. Мирошников Б.Н. Борьба с киберпреступлениями – одна из составляющих информационной безопасности Российской Федерации. [Електронний ресурс]. – Доступний з http://www.crime-research.org/library/Miros1.html

8. Політика інформаційної безпеки. [Електронний ресурс]. – Доступний з http://uk.wikipedia.org/wiki/Політика_інформаційної_безпеки.

9. Сташевський З.П. Особливості проблеми синтезу систем захисту інформації у структурних підрозділах МНС України / Сташевський З.П., Грицюк Ю.І.// Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2012. – Вип. 22.10. – С. 79-96.

З.П. Сташевский, О.И. Лозинский, Н.Э. Бурак

ВНЕДРЕНИЕ ПОЛИТИКИ РОЛЕВОГО РАЗГРАНИЧЕНИЯ ДОСТУПУ К ИНФОРМАЦИОННЫМ РЕСУРСАМ В СИСТЕМУ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Проведен анализ моделей существующих политик информационной безопасности как одной из основных составляющих системы защиты информации. На основе проведенного анализа определена наиболее оптимальная политика, основной функцией которой является защита информационных ресурсов (курсы учебных программ, личные данные пользователей, репозитарий и др.) системы дистанционного обучения "Виртуальный университет" Львовского государственного университета безопасности жизнедеятельности. Приведена модель ролевого разграничения доступа к этой учебной системе, которая дает возможность обеспечить надлежащий уровень защиты информации от внешних и внутренних угроз.

Ключевые слова: система дистанционного обучения, "Виртуальный университет", среда Moodle, политика безопасности, информационный ресурс, источники угроз.

Z.P. Stashevkyi, O.I. Lozynskyi, N.E. Burak

IMPLEMENTATION OF POLICY OF ROLE DIFFERENTIATION OF ACCESS TO INFORMATION RESOURCES IN DISTANCE EDUCATION SYSTEM

Existing models of information security policy as one of the main components of information security were analysed. Based on the analysis determined the optimal policy, whose main function is to protect information resources (courses training programs, personal user data repository, etc.) in distance education system "Virtual university" Lviv State University of Vital Activity Safety. Represents an effective model of role differentiation of access to this training system that helps ensure the proper level of information security against external and internal threats.

Key words: distance education system, "Virtual university", environment of Moodle, policy of safety, information resource, threat's sources.