УДК 316.74:378.147

О.І. Полотай, *канд. техн. наук*
Львівський державний університет безпеки життєдіяльності, м. Львів

Н.П. Кухарська, *кан.ф-м. наук*
Національний університет Львівська Політехніка

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ПОЛІТИКИ БЕЗПЕКИ ДИСТАНЦІЙНОГО КУРСУ

У статті розглядаються основні поняття інформаційної безпеки з точки зору дистанційного навчання. Описано особливості побудови політики інформаційної безпеки при роботі викладача-тьютора з дистанційним курсом. Показано основні загрози інформаційної безпеки дистанційного курсу. Розглянуто методи та засоби захисту інформації дистанційного курсу. Детально описано основні методи інформаційної безпеки дистанційного курсу, які реалізуються за допомогою основних засобів захисту. Запропоновано для учасників дистанційного навчання правила забезпечення політики безпеки дистанційного курсу.

Ключові слова: дистанційний курс, інформаційна безпека, політика безпеки

The article considers the basic concepts of information security in terms of distance learning. Features of construction of information security policy at work of the teacher-tutor with a distance course are described. The main threats to the information security of the distance course are shown. Methods and means of protection of distance course information are considered. The main methods of information security of the distance course, which are implemented with the help of basic means of protection, are described in detail. The rules of ensuring the safety policy of the distance course are offered for the participants of distance learning.

Key words: distance course, information security, security policy

Забезпечення інформаційної безпеки дистанційно курсу передбачає створення системи захисту його інформаційних ресурсів від зловмисників, які схочуть ці ресурси використовувати, модифікувати або просто знищити.

Під інформаційною безпекою розуміється «стан захищеності інформації, при якому забезпечені її конфіденційність, доступність та цілісність.

Комплексний характер, проблеми захисту говорить про те, що для її вирішення необхідне поєднання законодавчих, організаційних і програмно-технічних заходів.

Знання можливих загроз, а також вразливих місць інформаційної системи, необхідне для того, щоб вибирати найефективніші засоби забезпечення безпеки.

Одними з найнебезпечніших та найчастіших є ненавмисні помилки користувачів, операторів, системних адміністраторів і інших осіб, які обслуговують інформаційні системи. Іноді такі помилки призводять до прямих збитків (неправильно введені дані, помилка в програмі, що викликала зупинку або руйнування системи). Іноді вони створюють слабкі місця (найчастіше через помилки адміністрування), якими можуть скористатися зловмисники.

Друге місце за розмірами збитку посідають крадіжки і фальсифікації. В більшості випадків винуватцями виявлялися штатні співробітники організацій, чудово знайомі з режимом роботи і захисними заходами.

Ключовим етапом для побудови надійної інформаційної системи є вироблення політики безпеки. Є декілька визначень цього поняття. Наведемо деякі з них.

Політика безпеки – сукупність керівних принципів, правил, процедур і практичних прийомів в галузі безпеки, які регулюють управління, захист і розподіл цінної інформації.

Політика безпеки – це набір документованих норм, правил та практичних прийомів, що регулюють управління, захист та розподіл інформації обмеженого доступу.

З практичної точки зору політику безпеки доцільно розділити на три рівні:

- Рішення, що зачіпають організацію в цілому. Вони мають досить загальний характер і, як правило, йдуть від керівництва організації.

- Питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних систем, експлуатованих організацією.

- Конкретні методи для забезпечення інформаційної безпеки системи.

Ключовим моментом політики безпеки для системи дистанційного навчання є методи і засоби забезпечення захисту інформації та їх аналіз.

Методи можна класифікувати таким чином:

- перешкода;

- управління доступом;

- маскування;

- регламентація;

- примус;

- спонукання.

Розглянемо детальніше ці методи.

1. Перешкода – метод фізичного перешкоджання зловмиснику на шляху до захищуваної інформації.

2. Управління доступом – метод захисту інформації, пов'язаний з регулюванням використання всіх ресурсів інформаційної системи (елементів баз даних, програмних і технічних засобів).

Управління доступом включає такі функції захисту:

- ідентифікацію співробітників і ресурсів інформаційної системи;

- аутентифікацію (встановлення автентичності) об'єкта за пред'явленим ідентифікатором (іменем). Як правило, до таких засобів відносяться паролі;

- перевірку повноважень – авторизацію користувачів;

3. Маскування - метод захисту інформації шляхом її криптографічного закриття. Цей метод захисту широко застосовується за кордоном як при зберіганні інформації, так і при її обробці. При передаванні інформації каналами зв'язку великої протяжності цей метод є дійсно надійним.

4. Регламентація – метод захисту інформації, що створює певні умови автоматизованої обробки, зберігання та передаванні інформації, за яких можливість несанкціонованого доступу до неї (мережевих атак) зводиться до мінімуму.

5. Примус – метод захисту, при якому користувачі системи змушені дотримуватися правил обробки, передавання і використання захищуваної інформації під загрозою матеріальної, адміністративної та кримінальної відповідальності.

6. Спонукання – метод захисту інформації, який мотивує користувачів не порушувати встановлені правила шляхом дотримання сформованих моральних і етичних норм.

Всі названі методи інформаційної безпеки реалізуються за допомогою основних засобів захисту: фізичних, апаратних, програмних, апаратно-програмних, криптографічних, організаційних, законодавчих та морально-етичних.

Засоби забезпечення безпеки процесів переробки інформації, що використовуються для створення механізму захисту, поділяються на:

1. Формальні (виконують захисні функції за заздалегідь передбаченою процедурою без безпосередньої участі людини). До них належать:

- фізичні засоби захисту, які призначені для зовнішньої охорони території об'єктів і захисту компонентів інформаційної системи організації (механічні, електричні, електромеханічні, електронні, електронно-механічні пристрої та системи, які функціонують автономно);

- апаратні засоби захисту – це пристрої, які вбудовані в блоки інформаційної системи (сервери, комп'ютери і т.д.) або під’єднані до неї спеціально для вирішення завдань захисту інформації. Вони призначені для внутрішнього захисту елементів обчислювальної техніки та засобів зв'язку;

- програмні засоби захисту, що призначені для виконання функцій захисту інформаційної системи за допомогою програмних засобів (антивірусний захист, міжмережеві екрани і т.д.).

2. Неформальні (визначаються цілеспрямованою діяльністю людини або регламентують цю діяльність). До них належать:

- організаційні засоби – організаційно-технічні заходи, які спеціально передбачаються в технології функціонування системи з метою вирішення завдань захисту інформації;

- законодавчі засоби – нормативно-правові акти, які регламентують права та обов'язки, а також встановлюють відповідальність всіх осіб і підрозділів, що

мають відношення до функціонування системи, за порушення правил обробки інформації, наслідком чого може бути порушення її захищеності.

- морально-етичні засоби – притаманні суспільству або певному колективу моральні норми або етичні правила, дотримання яких сприяє захисту інформації, а порушення їх прирівнюється до недотримання правил поведінки в суспільстві або колективі.

Графічно така класифікація представлена на рис. 1.

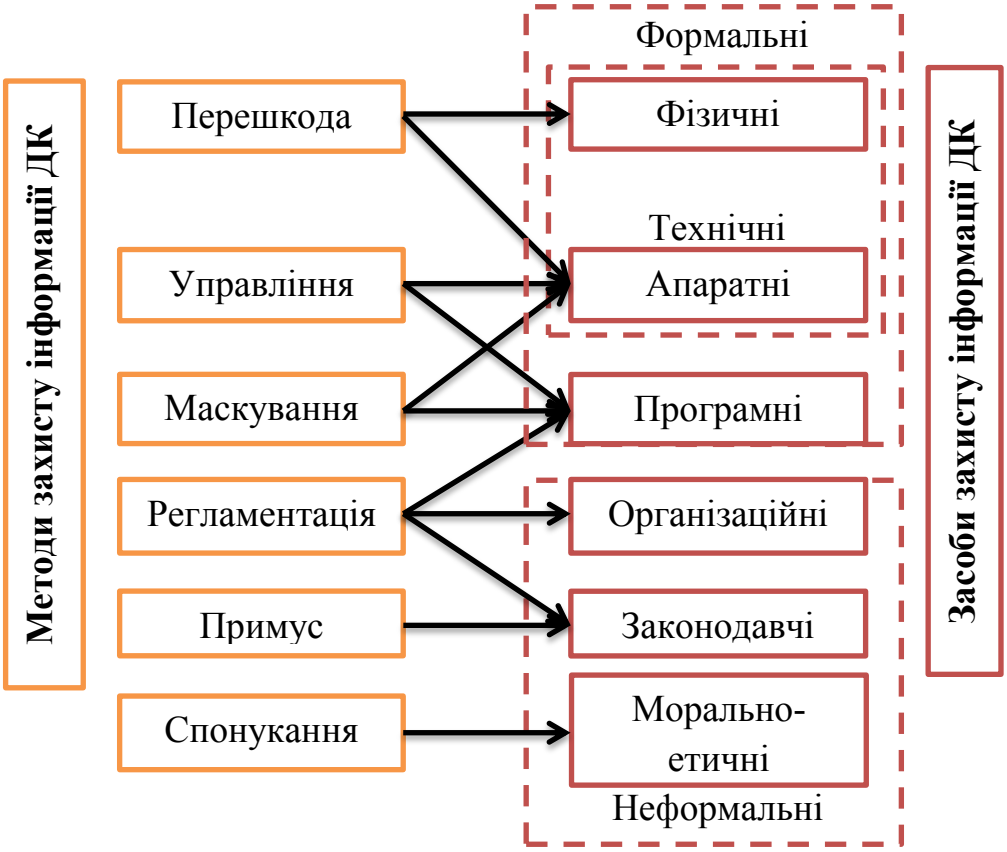

Рис. 1. Класифікація засобів безпеки процесів переробки інформації в дистанційному курсі

Політика інформаційної безпеки дистанційного курсу по відношенню до користувачів-студентів повинна бути доступною у кожному навчальному закладі і конкретизована у вигляді правил з інформаційної безпеки.

Необхідними заходами захисту дистанційного курсу навчального середовища від навмисних та ненавмисних дій студентів є: контроль з боку

адміністратора, персоналізація та обмеження доступу до критичних ресурсів, контроль і реагування на несанкціоновані дії програмних засобів захисту.

Основною метою політики безпеки дистанційного курсу є неухильне виконання користувачами-студентами правил інформаційної безпеки, які унеможливлюють чи зводять до мінімуму шкоду, яку вони можуть спричинити своїми діями. Ця мета реалізується організаційними, програмно-апаратними та виховними заходами.

До організаційних заходів належить розробка, впровадження та контроль за дотриманням політики безпеки системи інформаційної безпеки дистанційного курсу користувачами-студентами. Контроль за виконанням покладено на адміністратора.

Особливої уваги потребує проблема доступу користувачів-студентів до мережі Інтернет.

Правила щодо доступу в мережу Інтернет, встановлені в навчальному закладі, повинні бути формалізовані, тобто мати вигляд обов'язкового документа. Ці правила обов’язково мають включати інструкцію щодо публікації в мережі особистих даних студентів, їхніх фотографій, аудіо- і відеоматеріалів тощо.

Частина правил політики безпеки, що стосується доступу користувачів-студентів до мережі Інтернет, повинна бути повідомлена перед початком відповідних занять самим викладачем.

Програмно-апаратні засоби прийнятої політики безпеки реалізуються через систему управління (контролю) доступу користувачів до ресурсів, яка включає ідентифікацію та автентифікацію користувачів, управління (контроль) доступу до ресурсів, протоколювання та аудит дій користувачів. Програмно-апаратні засоби повинні гарантувати захищеність критично важливих компонентів програмного забезпечення навчального комп’ютерного комплексу від несанкціонованих і помилкових дій користувачів. В правилах розмежування доступу необхідно заборонити доступ цих користувачів до системних областей диска, а також заборонити модифікацію ними програмного забезпечення,

навчальної та іншої важливої інформації. Рекомендується надавати доступ до мережі Інтернет лише з тих комп'ютерів, які постійно перебувають у полі зору викладача. Також варто використовувати програми, що дають можливість відображати вміст екранів усіх комп'ютерів на моніторі викладача і тим самим дають змогу стежити за діями студентів.

Основними в реалізації політики безпеки дистанційного курсу навчального середовища є виховні заходи, оскільки вони використовуються як для запобігання несанкціонованого доступу, так і для впливу на порушників правил безпеки з метою їх перевиховання. Дуже важливо встановити правила покарання тих, хто зловживає доступом; порушення можуть бути і не настільки значними, але повинні бути обговорені, а за серйозні провини мають бути передбачені серйозні заходи покарання.

Головною метою виховних заходів є усвідомлення студентами відповідальності за свої дії навіть у віртуальному середовищі, засвоєння етичних норм поведінки в цьому середовищі, результатом чого є формування в студентів компетентності з інформаційної безпеки.

До методів, що використовуються для підвищення захищеності і відновлюваності програмної складової інформаційної системи дистанційного курсу, є резервування та періодична перевірка його цілісності. Ці методи можуть реалізовуватися системними утилітами, що входять до складу операційної системи або іншими програмами, наприклад, антивірусними.

Отже, проаналізувавши наведену вище інформацію, можна запропонувати наступні правила забезпечення політики безпеки дистанційного курсу:

1. Користувач типу адміністратор та викладач повинен мати пароль для свого облікового запису, який задовольняє встановленим вимогам;

2. Користувачі типу студент, гість, автентифікований користувач повинні мати мінімальний набір прав на роботу з електронним курсом.

3. Під час створення дистанційного курсу, та під час створення кожного електронного ресурсу, необхідно налаштовувати права на роботи з ним.

4. Після створення дистанційного курсу, необхідно створити його резервну копію.

5. Після створення дистанційного курсу необхідно налаштувати особливості реєстрації користувачів на нього та обов'язково відключити можливість самореєстрації на курс.

6. Під час роботи з дистанційним курсом, на персональному комп'ютері користувача необхідно активувати та оновити антивірусне програмне забезпечення, яке захистить від небажаних вірусів, що можуть пошкодити частину дистанційного курсу.

7. Після завершення терміну навчання на дистанційному курсі, викладач повинен очистити його від старої статистики, звітів, видалити всі виконані завдання, відрахувати з курсу усіх колишніх користувачів.

8. Після очищення дистанційного курсу, його необхідно приховати та закрити доступ студентів до нього.

Література:

1. Використання системи електронного навчання MOODLE для контролю і оцінювання навчальної діяльності студентів ВНЗ: методичний посібник / Ю.В. Триус, І.В. Стеценко, Л.П. Оксамитна, В.М. Франчук, І.В. Герасименко / За ред. Ю.В. Триуса. – Черкаси: МакЛаут, 2010. – 200 с.
2. Кухарська Н. П. Розробка політики інформаційної безпеки комп'ютерного контролю знань / Н. П. Кухарська // Вісник Львівського державного університету безпеки життєдіяльності. Львів: 2017, Том 16. – С. 34-39.
3. Офіційний сайт системи MOODLE [Електронний ресурс]. – Режим доступу: http://www.moodle.org
4. Полотай О.І.,Кухарська Н.П.Розроблення електронних курсів у віртуальному навчальному середовищі ЛДУ БЖД.Методичний посібник. – Львів, ЛДУБЖД, 2020. -172с.

5. Система електронного навчання ВНЗ на базі MOODLE: методичний посібник / Ю. В. Триус, І. В. Герасименко, В. М. Франчук // За ред. Ю. В. Триуса. – Черкаси. – 220 с.