ВИСВІТЛЕННЯ ПИТАНЬ ЗАХИСТУ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНОГО ПРОДУКТУ В ПРАКТИЧНІЙ ПІДГОТОВЦІ ДОКУМЕНТОЗНАВЦІВ

В. О. Ольховський, *к. т. н., доцент*
ВНЗ Укоопспілки «Полтавський університет економіки і торгівлі»

Технологічні, виробничі і комерційні дані підприємства мають високу вартість, а їх втрата або витік може призвести до фінансових втрат. Тому однією з цілей для підприємства є захист інформації. Але на малих підприємствах утримання штатного співробітника або відділу по інформаційній безпеці еконо-мічно невиправдане. У таких випадках випускник-документознавець ПУЕТ на посаді секретаря-референта, як помічник керівника, має бути підготовлений в питаннях забезпечення інформаційної безпеки підприємства. Він має бути готовий дати загальні рекомендації керівнику підприємства в питаннях захисту інформації, а при необхідності організувати роботу діловодства з урахуванням вимог по інформаційній безпеці.

Система захисту інформації – це комплекс організаційних і технічних заходів, які забезпечують інформаційну безпеку підприємства. Об'єктом захисту є дані, що обробляються в системі управління. Основні загрози для інформаційної безпеки компанії пов'язані з крадіжкою даних, використанням хибного програмного забезпечення (з вірусами), атаками хакерів, отриманням спаму (з вірусами), халатністю співробітників. Втрату даних можуть викликати збої в роботі апаратно-програмного забезпе-чення, крадіжки устаткування або техногенні та стихійні лиха. Випускник ПУЕТ повинен знати заходи протидії таким загрозам і вміти організувати роботу по захисту критичних даних підприємства.

Процес створення системи захисту інформації містить етапи:

Процес створення системи захисту інформації містить етапи:

- формування політики інформаційної безпеки підприємства;
- вибір і впровадження технічних і програмних засобів захисту;
- розробка і проведення низки організаційних заходів.

Юридичною основою системи захисту інформації на підприємстві є «Політика підприємства в області інформаційної безпеки». Це система нормативно-правових документів, які визначають правила забезпечення інформаційної безпеки на підприємстві та встановлюють відповідальність за їх порушення. До складу правового забезпечення включаються державні закони і акти, нормативні і організаційні документи підприємства. Випускник повинен вміти розробити такі документи і стежити за дотриманням їх вимог.

Виходячи з аналізу загроз втраті даних випускник повинен вміти визначати основні напрями забезпечення інформаційної безпеки. При вирішенні цієї задачі визначаються компоненти системи управління, які потребують захисту, обираються необхідні програмні і технічні засоби, формулюються організаційні заходи, направлені на захист інформації.

Технічні і програмні засоби захисту інформації в системі управління діляться на три групи – для захисту змісту даних, забезпечення збереження інформації при форс-мажорних обставинах і усунення можливості несанкціонованого доступу до ресурсів системи. Практичні вміння і навички випускника-документознавця повинні охоплювати ці три напрями.

Для захисту змісту даних застосовують технології шифрування і електронний цифровий підпис, що дозволяє досягти конфіденційності і цілісності інформації, її однозначної аутентифікації. Програма підготовки містить практичні заняття по шифруванню документів засобами MS Office, програмами сторонніх розробників.

Збереження даних при позаштатних ситуаціях забезпечується засобами резервного копіювання. На практичних заняттях студенти створюють резервні копії документів і каталогів та відновлюють їх за допомогою відповідного програмного і апаратного забезпечення, у тому числі і з використанням хмарних технологій.

Запобігання несанкціонованому доступу до інформації забезпечується захистом персональних комп'ютерів, серверів і мережевих з'єднань. Для цього застосовуються методи парольної ідентифікації операційної системи Windows, BIOS або додаткові програмні компоненти. Спеціальні програми журналювання контролюють дії користувачів із запуску додатків і звернення до даних, а всі операції фіксуються в журналі, доступ до якого має тільки системний адміністратор, відповідальний за інформаційну безпеку. Захист мережевих з'єднань забезпечується за допомогою технологій міжмережевого екранування. Міжмережеві екрани ведуть моніторинг даних, що поступають із зовнішнього середовища, і оцінюють їх на предмет загрози для внутрішньої мережі підприємства.

Організаційні заходи щодо захисту інформації зазвичай включають розробку інструкцій для співробітників, організацію окремої структури захищеного документообігу для конфіденційних документів, охорону приміщень і розробку пропускного режиму, проведення перевірок дотримання правил інформаційної безпеки.

За рахунок застосування програмних і апаратних засобів, виконання організаційних заходів забезпечується збереження даних, які обробляються в автоматизованій системі управління, і мінімізуються ризики втрати інформації на підприємстві.