УДК 621.326
Гнатишин М. – ст. гр. СН-51
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ ВУЗІВ

Науковий керівник: доцент кафедри КН Марценко С. В.

Збільшення кількості сервісів і нових інформаційних технологій в освітньому процесі та системах управління вузом, створило передумови до появи корпоративних мереж. Оскільки такі мережі зазвичай об'єднують не тільки структурні підрозділи вузу із великою кількістю користувачів, але і їх регіональні представництва, виникає проблема інформаційної безпеки цих мереж.

Проблеми комплексної інформаційної безпеки корпоративних мереж вузів набагато ширші, різноманітніші і гостріші, ніж в інших системах. У такій мережі можливі як внутрішні, так і зовнішні загрози безпеки інформації, а саме:

- спроби несанкціонованого адміністрування баз даних, які містять конфіденційну інформацію;
- дослідження мереж у зловмисних цілях;
- видалення інформації;
- встановлення вірусних програм і троянських коней;
- DoS-атаки на сервери;
- спроби злому автоматизованої системи керування вищого навчального закладу;
- використання мережевих ресурсів для злому мережі інших організацій;
- спроби проникнення в системи бухгалтерського обліку;
- пошук “дірок” в ОС, Firewall, Proxy-серверах;
- спроби несанкціонованого віддаленого адміністрування ОС і т.д.;

Таким чином, результатом реалізації загрози безпеці інформації в мережі може бути витік (копіювання) інформації, її втрата (руйнування) або спотворення (підробка), блокування інформації.

Для вирішення поставленої задачі, система комплексної інформаційної безпеки повинна включати в себе політику безпеки, що передбачає наступні кроки:

- захист. Повинен обов’язково включати в себе аутентифікацію, шифрування, між мережеві екрани.
- моніторинг і реагування. Повинні виявляти порушення політики безпеки; виконувати нагляд за системи виявлення вторгнень у реальному часі; підтверджувати реалізацію безпеки на попередньому кроці.
- тестування. Визначення ефективності політики безпеки шляхом системного аудиту і сканування мережі для визначення уразливостей.
- покращення. Використання інформації, отриманої на етапах моніторингу та тестування, для поліпшення реалізації безпеки; підстроювання політики безпеки у випадку виявлення ризиків та уразливостей.

Отже, захист мережі як єдиної системи складається із заходів захисту кожного окремого вузла і функцій захисту протоколів даної мережі.

Так само, можна зробити висновок про те, що оскільки складно заздалегідь, визначити можливу сукупність загроз безпеки інформації і результатів їх реалізації, модель потенційних загроз безпеці інформації в корпоративній мережі повинна створюватися спільно власником мережі та фахівцями з захисту інформації на етапі проектування мереж. Створена модель повинна потім уточнюватися в ході експлуатації корпоративної мережі.

Недооцінка цих напрямків буде компенсуватися підвищеними фінансовими витратами на супровід корпоративних мереж вузів.