– Даст возможность абоненту получить большой пакет услуг по низкой цене
– Позволит увеличить гибкость использования существующих систем связи
– Улучшить использование радиочастотного спектра.

Основные недостатки:

Основной недостаток – это большое энергопотребление.

Таблица

Сравнительная таблица стандартов беспроводной связи

Технология	Стандарт	Пропускная способность	Радиус действия	Частоты
Wi-Fi	802.11a	До 54 Мбит/с	До 300 метров	5,0 ГГц
Wi-Fi	802.11b	До 11 Мбит/с	До 300 метров	2,4 ГГц
Wi-Fi	802.11g	До 54 Мбит/с	До 300 метров	2,4 ГГц
Wi-Fi	802.11n	До450Мбит/с	До 300 метров	2,4-2,5 или 5,0 ГГц
WiMAX	802.16d	До 75 Мбит/с	25-80 км	1,5-11 ГГц
WiMAX	802.16e	До 40 Мбит/с	1-5 км	2,3-13,6 ГГц
3GPP LTE	LTE (2x2MIMO)	До 173 Мбит/с	До 100км	698 МГц – 3500 МГц
3GPP LTE	LTE (4x4MIMO)	До 326 Мбит/с	До 100 км	698 МГц – 3500 МГц

І. Попазов,
студент 5 курсу факультету
Комп'ютерних наук та інноваційних технологій,
Міжнародний гуманітарний університет;
керівник – канд. техн. наук, проф. В. Г. Головань

ЗАХИСТ ІНФОРМАЦІЇ В ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ НАВЧАЛЬНОГО ЗАКЛАДУ

Розвиток інформаційних технологій привів до масового використання комп'ютерної техніки у різних галузях суспільства. Одним із напрямів державної політики щодо розвитку вищої освіти є впровадження освітніх інновацій та інформаційних технологій, які забезпечують:

- доступність та ефективність освіти;
- удосконалення навчально-виховного процесу;
- підготовку молоді до життєдіяльності в інформаційному суспільстві.

Саме інформаційні технології «забезпечують учням і студентам вільний

доступ до різноманітної інформації, набуття навичок вирішення різноманітних проблем на основі їх всебічного дослідження і аналізу, здобуття певних знань в різноманітних галузях» [1, с. 16–17].

З метою удосконалення організації навчального процесу, підвищення якісного рівня підготовки фахівців створюються навчальні комп'ютерні лабораторії. Діяльність таких лабораторій спрямована на якісне забезпечення навчального процесу, зокрема про-

ведення лабораторних занять з використанням комп'ютерної техніки та спеціальних програм, а також створення умов для забезпечення науково-дослідної роботи викладачів, аспірантів, студентів усіх форм навчання. Ці лабораторії оснащені комп'ютерною технікою з'єднаною у локальну мережу з вільним доступом до мережі Internet. Основна проблема при використанні комп'ютерних мереж – атаки на локальну мережу. Тому актуальною на даний момент є проблема захисту інформації комп'ютерних мереж від несанкціонованого доступу.

Сучасна мережа передачі даних це безліч віддалених високопродуктивних пристроїв, що взаємодіють один з одним на деякій відстані. Однією з найбільш великомасштабних мереж передачі даних є комп'ютерна мережа Internet. У ній одночасно працюють мільйони джерел і споживачів інформації по всьому світу. Разом з тим, загальний доступ до єдиних фізичних ресурсів відкриває доступ шахраям, вірусам та конкурентам, а це надає можливість заподіяти шкоду кінцевим користувачам: викрасти, спотворити, модифікувати, знищити збережену інформацію, порушити цілісність програмного забезпечення і навіть вивести апаратну частину кінцевої станції. Через мережу Internet порушник може:

- вторгнутись у внутрішню мережу навчального закладу та отримати несанкціонований доступ до інформації;
- незаконно скопіювати важливу і цінну інформацію;
- отримати паролі, адреси серверів, а часом і їх вміст;
- входити в інформаційну систему навчального закладу під ім'ям зареєстрованого користувача.

Для запобігання небажаних впливів варто використовувати міжмережеві екрани (Firewall, Brandmauer, брандмауер). Сам термін «брандмауер» запозичений з німецької мови, що у дослівному перекладі означає «стіна, яка розділяє суміжні будівлі, оберігаючи від поширення пожеж» є аналогом англійського слова «firewall». Слово «фаєрвол» утворено транслітерацією англійського терміна «firewall» і означає «вогняна стіна», який є еквівалентний терміну «міжмережевий екран» [2]. Міжмережевий екран служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Він призначений для контролю вхідного і вихідного трафіку на комп'ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, вспливаючі вікна та інше, не надсилати іншим «чужим» серверам інформацію про ваш комп'ютер,робить даремною роботу програм-троянів і засобів віддаленого адміністрування [3].

Література

1. Кремень В. Г. Освіта і наука в Україні : інноваційні аспекти. Стратегія. Реалізація. Результати / В. Г. Кремень. – К. : Грамота, 2005. – 448 с.

2. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Изд-во НиТ, 2004. – 384 с.

3. Меншиков В. Р. Защита информации в компютерных сетях / В. Р. Меншиков – М. : Финансы и статистика, 1997. – 432 с.