Для зручної навігації по електронному посібнику використовуються гіперпосилання, що допомагає швидко знайти необхідну інформацію(презентація), у тому числі контекстний пошук, істотно заощаджує час при багаторазових звертаннях до гіпертекстових пояснень.

Головна перевага електронного підручника – можливість інтерактивної взаємодії студента з матеріалом підручника.

Створення електронного посібника – це творчий процес викладача і програміста(презентація програм).

Результат виконаної роботи - електронний підручник з фізики, застосований для використання студентами І курсу в процесі аудиторного навчання, самостійної роботи та поглиблення знань(презентація). Він не володіє високим дизайном, однак дає можливість включити мультимедійні способи представлення інформації, інтерактивні моделі та тестовий контроль, дає можливість гнучкої корекції методичних матеріалів і дидактичного доповнення відповідно до змін в навчальних програмах, до речі, які відбуваються останнім часом кожного року. Тому ми доповнили електронний варіант підручника конспектами занять, матеріалами для самостійної роботи студентів, зразками розв'язання типових задач, питаннями до самоперевірки, в ньому знаходиться тематичний план вивчення дисципліни, збірник задач та додаткові матеріали з предмету, інструкції до лабораторних робіт, мультимедійна бібліотека, тощо, які переростають в окремий завершений електронний навчально-методичний комплекс(презентація структурної схеми).

Керівники: Романенко О.І., Комісаренко Н.І., *викладачі*

ЗАХИСТ ПУНКТІВ ЕЛЕКТРОННОЇ ПОШТИ

Удот А. В., *студент*; Малишок Є.О., *студент*
Шосткінський інститут СумДУ

При створенні системи електронної пошти спеціального призначення із абонентськими пунктами на основі ЕОМ у захищеному виконанні для обробки, прийому, перетворення, зберігання, відображення і передачі (надалі - "обробки") інформації з обмеженим доступом використання засобів криптозахисту викликано, у тому

числі, можливістю застосування у ряді випадків для зв'язку між абонентами незахищених ліній.

Сучасні криптосистеми забезпечують достатню стійкість перехопленого повідомлення до дешифрування. Проте стійкість системи різко знижується, якщо є можливість перехоплення ключів від шифру, або незашифрованого повідомлення разом із зашифрованим, або хоча б їх частин. Ці відомості можуть бути перехоплені технічними засобами за наявності, наприклад, в кінцевих пристроях обробки інформації каналів її витоку за рахунок побічних електромагнітних випромінювань і наводів (ПЕМВН). При введенні в ЕОМ з клавіатури необхідних для шифрування інформації даних вони можуть бути перехоплені на достатньо великих відстанях, до сотень і навіть тисяч метрів. Так само може бути перехоплена і інформація, яка обробляється в системному блоці або відображується на екрані монітора. Таким чином, застосування криптографічних засобів захисту інформації має сенс лише при неможливості перехоплення інформації по ПЕМВН в кінцевих пунктах зв'язку.

На підставі викладеного слід зазначити, що абонентські пункти електронної пошти спеціального призначення з використанням криптосистем вимагають гарантованого захисту оброблюваної інформації від перехоплення по ПЕМВН, зокрема, при її введенні-виведенні, кодуванні-декодуванні, виробленні-перевірці електронного цифрового підпису і т.п. Рівень захисту інформації ЕОМ таких абонентських пунктів повинен відповідати вимогам захищеності інформації на об'єктах першої категорії, для чого необхідно застосовувати екрановані приміщення або ЕОМ у захищеному виконанні, створені для об'єктів цієї категорії.

Запобігання витоку інформації за рахунок ПЕМВН є важливою складовою частиною забезпечення стійкості криптографічної системи. Саме тому і західні фірми, які поставляють криптографічні системи високої стійкості, вимагають захисту інформації від витоку по ПЕМВН на кінцевих пристроях на рівні норм по так званій "нульовій зоні".

Крім того, інформація в абонентських пунктах електронної пошти на основі ЕОМ в захищеному виконанні з використанням криптосистем повинна бути захищена не тільки від витоку по ПЕМВН, але і від витоку каналами електроакустичного перетворення,

високочастотного нав'язування і опромінювання.

Використання в системах зв'язку з криптозахистом генераторів шуму як технічних засобів захисту інформації від перехоплення по ПЕМВН не ефективне, оскільки сучасні засоби цифрової обробки і оптимальної фільтрації дозволяють розпізнавати сигнали, рівень яких значно нижчий рівня маскуючих шумів цих генераторів.

Існуючі зразки генераторів шуму забезпечують перекриття діапазону частот від декількох десятків або сотень кілогерц до одного-півтора гігагерц, не перекриваючи при цьому діапазон хоча б третьої - п'ятої ("червоних") гармонічних складових тактових частот сучасних ЕОМ. При цьому для високочастотної частини діапазону характерна значна залежність рівня шумового сигналу від місцевих умов, тобто значна просторова нерівномірність, що дозволяє використовувати просторову селекцію і тим самим ліквідовувати маскуючу дію генератора.

Крім того, підвищення рівня електромагнітного шуму до величини не менше 50-60 дБ, особливо в діапазоні вищих гармонічних складових інформативних сигналів, неприпустимо за рівнем радіоперешкод (по ГОСТ 29216-91 - не більше 37 дБ), і небажано з погляду впливу на здоров'я операторів. Наприклад, вмикання і вимикання генераторів шуму легко визначається за самопочуттям.

Робота генератора шуму з метою ТЗІ до того ж демаскує місцезнаходження об'єкту і час обробки інформації, що захищається, а можливість попереднього запису інформаційних сигналів ЕОМ (спектр цих сигналів не залежить від грифа секретності оброблюваної інформації) при вимкненому генераторі шуму полегшує подальше виділення інформаційних сигналів з-під маскуючих шумів.

Але найважливішим, на наш погляд, недоліком генераторів шуму, разом з можливістю застосування просторової селекції, є небезпека модуляції їх випромінювання (як і будь-якого іншого генератора) якраз тими інформаційними сигналами, які вони повинні захищати, тобто цей засіб "захисту" насправді може забезпечувати витікання інформації. Рівень сигналу генератора шуму значно перевищує рівень інформаційних сигналів незахищеної ЕОМ. При цьому створюється ефективний канал витоку, оскільки використовується самий перешкодостійкий спосіб передачі інформації із застосуванням шумоподібних сигналів, і дальність виявлення таких сигналів може

бути значно більшою, ніж сигналів ЕОМ в незахищеному виконанні.

Використання генераторів шуму як засобів ТЗІ створює у споживача помилкове уявлення щодо захищеності оброблюваної інформації і приводить до даремної витрати коштів. Отже, генератори шуму можуть застосовуватися хіба що на "побутовому рівні", і не повинні використовуватися для захисту інформації, необхідність захисту якої визначена законодавством України.

Необхідний рівень захисту інформації забезпечує розміщення абонентних пунктів в екранованих приміщеннях, але це вимагає значних витрат на їх створення і експлуатацію.

В той же час екрановані приміщення небезпечні для здоров'я внаслідок ізоляції людини від природного середовища і заміни його на несприятливі, через електромагнітне опромінювання, умови. Це додатково поглиблюється наявністю відбивання, перевідбивання і складання між собою випромінювань від різних засобів обчислювальної техніки (ЗОТ) і металевих конструкцій, у тому числі від корпусів системних блоків ЕОМ, серверів і поверхонь електромагнітних екранів, розташованих в такому приміщенні, навіть у разі використання ЗОТ, які за рівнем випромінювання відповідають ТСО-99.

Таким чином, для забезпечення необхідного рівня біологічного захисту людей, що працюють в екранованих приміщеннях, слід використовувати ЗОТ в захищеному виконанні і в таких приміщеннях, що приведе, у свою чергу, до ще більшого порожчання останніх.

Керівник: Булашенко А.В., Забегалов І.В, *викладач*

УЧБОВИЙ ЦЕНТР «БЕРЕГИНЯ». ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ПРОДУКТІВ В ОСВІТНЬОМУ ПРОСТОРІ

Тукман Є.В., Дерезюк О.О., Батечко Ю.О., Чмутенко Н.В.,
Скубко О.С., Усенко Н.В., *студенти*
Індустріально-педагогічний технікум КІ СумДУ

Сучасні суспільні, соціально-економічні та інформаційно-технологічні зміни висувають нові вимоги до підготовки вчителя нової генерації, що потребує створення й застосування нових освітніх систем, зміни освітнього процесу, форм, методів та засобів навчання. Виникає