та завантажують в сушильну камеру. За умови, що температура вимикання ІЧ-випромінювачів 55…60 ^{o}С, а вмикання 45…50 ^{o}С. Щільність потоку випромінювання 12 кВт/м^2, діапазон довжин хвиль 9 мкм. Тривалість включення ІЧ-випромінювачів 3…10 с. Процес сушіння завершувався за умов досягнення матеріалом залишкової вологості 8%. За органолептичними показниками петрушка після сушіння відповідала ГОСТу Р52622-2006 та зберігала 70…85% вітамінів.

Переваги запропонованого способу сушіння рослинної капілярно пористої сировини полягають у:

– забезпеченні максимально рівномірного розподілу теплових потоків на приймальні поверхні (піддони) із сировиною за рахунок запропонованої для реалізації цього способу ІЧ-сушарки, а також геометрії її робочої камери та розміщення ІЧ-випромінювачів;

– зменшенні енерговитрати, підвищенні якості отриманої продукції та прискоренні процесу сушіння за рахунок застосування запропонованої ІЧ-сушарки та імпульсного режиму нагрів-охолодження;

– забезпеченні використання вторинного (нагрітого) повітря, для інтенсифікації процесів сушіння за рахунок створення турбулентного режиму в пристінному шарі біля ІЧ-випромінювачів із попереднім підігріванням свіжого повітря.

Список використаних джерел:

1. Сажин Б. С. Сучасні методи сушки / Б.С. Сажин. – М .: Знання, 1973 г. – 216 с.

2. Лыков М. В. Сушка в химической промышленности / М.В. Лыков. – М.: Химия, 1970. – 428 с.

3. Пат. 90104 Україна, A23B 7/028 B01D 1/22. ІЧ-сушарка органічної рослинної сировини / Черевко О.І., Кіптела Л.В., Загорулько А.М.; заявник Черевко О.І., Кіптела Л.В., Загорулько А.М., власник ХДУХТ; – № u 2013 14950; заявл. 20.12.2013; опубл. 12.05.2014, Бюл. № 9. – 3 с.

Кифик І.І., Соломончук А.С.

магістри,

Науковий керівник: **Кузьміна О.М.**

кандидат технічних наук, доцент,

Вінницький торговельно-економічний інститут

Київського національного торговельно-економічного університету

СУЧАСНІ ЗАСОБИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ НА ПІДПРИЄМСТВІ

На сьогоднішній день в Україні та усьому світі швидкими темпами впроваджуються новітні досягнення комп`ютерних і телекомунікаційних технологій, в зв’язку з цим збільшився відсоток несанкціонованого використання даних та інформації. Тому досить актуальним є питання щодо забезпечення необхідного рівня захисту інформації.

Питанню захисту інформаційних систем приділяють велику увагу такі вчені: Г. Кіссінджер, З. Бжезинський, Л. Браун, Ч. Флавін, Х. Френч, О. Сосніна, В. Грубова, В. Домарьова, В. Ліпкана, В. Косевцова, І. Бінько, В. Мунтіяна, Г. Почепцова, О. Литвиненко та інші.

Інформаційна безпека підприємства ─ це захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Виділяють чотири основні дії, які можуть завдати шкоди інформаційній безпеці підприємства, а саме:

1. Дії, які здійснюються авторизованими користувачами. У цю категорію потрапляють: цілеспрямована крадіжка або знищення даних на робочій станції або сервері; пошкодження даних користувачів у результаті необережних дій;

2. «Електронні» методи впливу, які здійснюються хакерами. До таких методів відносяться: несанкціоноване проникнення в комп'ютерні мережі, DOS атаки – розподіленої мережевої атаки, яка за допомогою численної кількості джерел має на меті порушити доступність сервісу (автоматизованої системи) шляхом вичерпання його обчислювальних ресурсів.

3. Комп'ютерні віруси. Окрема категорія електронних методів впливу – комп'ютерні віруси та інші шкідливі програми, такі як: мережеві хробаки – підклас вірусів, що інфікують комп'ютери та шукають способи для розповсюдження по мережі, створюючи свої копії; троянські програми – програми, призначенні для прихованого (під виглядом чогось іншого) проникнення до системи, зазвичай, зі зловмисними намірами; руткіти – набір програм, призначених для для приховування факту «присутності» зловмисників у системі (комп'ютері); клавіатурні шпигуни – забезпечують фіксацію всіх переривань, що надходять у систему вводу під час натискання клавіш на клавіатурі;

4. «Природні» загрози. На інформаційну безпеку компанії можуть впливати різноманітні зовнішні фактори. Так причиною втрати даних може стати неправильне зберігання, крадіжка комп'ютерів і носіїв, форс-мажорні обставини і т.д [1].

На сьогоднішній день експерти в галузі захисту інформаційної безпеки виділяють такі методи:

─ засоби ідентифікації і аутентифікації користувачів (так званий комплекс 3А);

─ засоби шифрування інформації, що зберігається на комп'ютерах і що передається по мережах;

─ міжмережеві екрани;

─ віртуальні приватні мережі;

─ засоби контентної фільтрації;

─ інструменти перевірки цілісності вмісту дисків;

─ засоби антивірусного захисту (користуватися антивірусним програмним забезпеченням та регулярно оновлювати бази даних сигнатур вірусів);

─ системи виявлення вразливостей мереж і аналізатори мережевих атак (при користуванні Інтернет-ресурсами (соціальні мережі, системи обміну повідомленнями, новини, онлайн-ігри) не переходити по невідомих посиланнях

та не завантажувати файли, що мають потенційно небезпечне розширення (наприклад, .exe, .bin, .ini, .dll, .com, .sys, .bat тощо). [1]

Отже, у сучасних умовах надійне забезпечення інформаційної безпеки є неодмінною умовою функціонування підприємства, адже від цього залежить його успіх в подальшому. Тому, що впровадження сучасних інформаційних технологій дозволяє скоротити час, необхідний на підготовку конкретних маркетингових і виробничих проектів, зменшити непродуктивні витрати при їх реалізації, виключити можливість появи помилок у підготовці бухгалтерської, технологічної та інших видів документації, що дає комерційної компанії прямий економічний ефект.

Список використаних джерел:

1. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: Учебное пособие.2-е изд. ─М.: Издательско-торговая корпорация «Дашков и К°». 2005. –336 с.

2. Живко М. О. Захист інформації: правовий аспект і проблематика // Інформаційна безпека. – 2010. – № 1.

3. Ігнатьєва О. В. Інформаційна безпека й основні загрози захисту комп'ютерів // – Інформаційна безпека . – 2010. – № 2.

Ковтюх А.С.

студент;

Яшков І.О.

доцент,

Научный руководитель: **Роменский В.И.**

доцент,

Харьковский национальный университет радиоэлектроники

ОСОБЕННОСТИ АВТОМАТИЧЕСКОГО МНОГОФУНКЦИОНАЛЬНОГО ЗВОНКА

Сегодня с помощью интенсивного использования электроники и микропроцессорной техники можно реализовать предлагаемый в данной работе автоматический много функциональный звонок. Для этого можно использовать процессор Intel 8080, но при этом будут иметь место такие недостатки: сложность и высокая стоимость самого устройства. Использование процессора Intel 8080 предполагает так же наличие внешней ПЗУ и ОЗУ. Кроме того, их необходимо подключить к процессору. При использовании такого процесора будет существовать необходимость замены самих звонком на динамики. Совершенно ясно, что это затратное мероприятие. Существует необходимость проектирования и изготовления усилителя, так как выход микросхемы не может дать необходимую мощность.Следует отметить сложность программного алгоритма. Реализация более дружественного звучания звонка потребует значительного усложнения используемого оборудования и программного обеспечения для его выполнения.

Предлагается техническое решение, которое лишено выше перечисленных недостатков. За счёт использования микроконтроллера отпала необходимость использовать внешнюю память, так как память уже встроена в сам контроллер.