

4. Візуалізація процесу складання схеми та роботи з вимірювальними приладами.
5. Розвиток логічного мислення, зумовлений необхідністю здійснення порівняльного аналізу отриманих розрахункових даних та визначених за допомогою віртуальних вимірювальних приладів.

Література

1. Ладогубець Н.В. Аналіз вибору передумов оптимальності навчального процесу бакалаврів у вищій технічній школі / Н.В. Ладогубець // Теорія і практика педагогічного процесу : зб. наук. праць. – Харків : Вид-во "Каравела", 2000. – С. 60-66.
2. Щерба А.А. Електротехніка. Лінійні кола : лаборат. практик. / А.А. Щерба, І.А. Петренко. – К. : Вид-во НТТ України "КПІ", 2007. – 140 с.
3. Офіційний сайт компанії NI. [Електронний ресурс]. – Доступний з <http://www.ni.com/multisim/>.
4. Шегедин О.І. Теоретичні основи електротехніки / О.І. Шегедин, В.С. Маляр. – Львів : Вид-во "Магнолія плюс", 2004. – Ч. 1. – 169 с.

Цыбуляк Б.З. Моделирование линейных электрических цепей постоянного тока

Рассмотрены аспекты использования компьютерных технологий в учебном процессе Львовского государственного университета безопасности жизнедеятельности для преподавания ряда технических дисциплин. Разработаны методические указания к лабораторной работе по исследованию электрических цепей постоянного тока с использованием законов Кирхгофа на базе программного обеспечения NI Multisim. Проанализированы преимущества использования виртуальной лаборатории для моделирования работы электрических цепей.

Ключевые слова: информационные технологии, моделирование, электрическая схема, закон Кирхгофа, Multisim.

Tsybulyak B.Z. Simulation of linear electric DC circuits

The aspects of using computer technologies in educational process Lviv State University of Vital Activity Safety while teaching a several of technical disciplines are considered. Guidelines for laboratory studies of DC circuits using Kirchhoff's laws were created using the software NI Multisim. The advantages of using a virtual laboratory for simulating the processes in electrical circuits was analyzed.

Keywords: information technology, simulation, electrical circuit, Kirchhoff's circuit law, Multisim.

УДК 65.012.8

*Проф. С.В. Васильчак, д-р екон. наук;
магістрант О.В. Байдак – Львівський ДУВС*

ПОРЯДОК АТЕСТУВАННЯ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Усі суб'єкти системи технічного захисту інформації, які здійснюють свою діяльність у сфері технічного захисту інформації, мають проходити відповідну атестацію. Проаналізовано процес атестування системи технічного захисту інформації: етапи побудови моделі загроз інформації, види атестування, порядок здійснення та терміни його проведення, розглянуто об'єкти та суб'єкти атестування.

Вступ. Функціонування системи технічного захисту інформації здійснюється з урахуванням необхідності гарантування відповідності рівня захищеності інформації вимогам нормативних документів. При цьому належну якість робіт із технічного захисту інформації можна забезпечити за умови за-

лучення висококваліфікованих спеціалістів, які мають відповідну фахову підготовку та досвід роботи, за відповідного технічного оснащення.

З урахуванням зазначеного, всі суб'єкти системи технічного захисту інформації, які здійснюють свою діяльність у сфері технічного захисту інформації, мають проходити відповідну атестацію: суб'єкти господарської діяльності отримують ліцензію відповідно до Закону України "Про ліцензування певних видів господарської діяльності". Наразі в Україні здійснюють діяльність близько 230 ліцензіатів у сфері технічного захисту інформації, а державні органи мають дозволи на право виконання робіт з технічного захисту інформації для власних потреб.

Метою нашого наукового дослідження є обстеження об'єктів інформаційної діяльності та визначення об'єктів захисту, виявлення загроз, їхній аналіз та формування окремої моделі загроз.

Виклад основного матеріалу. Обстеження має здійснювати комісія, склад якої визначає відповідальна за технічний захист інформації особа і затверджується наказом керівника.

У ході обстеження потрібно:

- проаналізувати умови функціонування об'єктів інформаційної діяльності, їх розташування на місцевості (ситуаційний план) для визначення можливих джерел загроз;
- дослідити засоби забезпечення об'єктів інформаційної діяльності, радіус дії яких виходить за межі контрольованої території;
- передбачити вивчення схем засобів і систем життєзабезпечення об'єктів інформаційної діяльності (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій;
- дослідити інформаційні потоки, технологічні процеси передавання, одержання, використання, розповсюдження і зберігання інформації;
- визначити наявність та технічний стан засобів забезпечення технічного захисту інформації;
- перевірити наявність на об'єктах інформаційної діяльності нормативних документів, які забезпечують функціонування системи захисту інформації, а також нормативної та експлуатаційної документації, яка забезпечує інформаційну діяльність;
- виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у канали) кабелів і провідників;
- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою необхідністю і які підлягають демонтажу;
- визначити технічні засоби, які потребують переобладнання (перемонтування) та встановлення засобів технічного захисту інформації.

За результатами обстеження потрібно скласти акт, який повинен затвердити керівник. Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна охоплювати:

- генеральний та ситуаційний плани, схеми розташування засобів і систем забезпечення інформаційної діяльності, а також інженерних комунікацій, які виходять за межі контрольованої території;
- схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до інформації з обмеженим доступом;
- оцінювання збитків, які передбачаються від реалізації можливих загроз.

Для визначення повноти та якості робіт з технічного захисту інформації потрібно здійснити атестування об'єктів інформаційної діяльності. Атестування виконують організації, які мають ліцензії на право діяльності в галузі технічного захисту інформації.

Об'єктами атестування є системи забезпечення інформаційної діяльності та їхні окремі елементи, де циркулює інформація, яка підлягає технічному захисту. У ході атестування потрібно:

- встановити відповідність об'єкта інформаційної діяльності, який атестується, вимогам технічного захисту інформації;
- оцінити якість та надійність заходів захисту інформації;
- оцінити повноту та достатність технічної документації для об'єкта атестування;
- визначити необхідність внесення змін і доповнень до організаційно-розпорядчих документів тощо.

Порядок атестування встановлюють нормативні документи системи технічного захисту інформації. Атестування комплексу технічного захисту інформації здійснюється за відповідними програмою і методиками випробувань. На підставі результатів випробувань складають висновок щодо відповідності стану технічного захисту інформації вимогам нормативних документів. Атестування може бути первинним, поточним та позачерговим. Первинне атестування здійснюють після (або під час) приймання робіт із створення комплексу технічного захисту інформації.

Термін проведення поточного атестування визначається технічним паспортом на комплекс технічного захисту інформації або актом попереднього атестування. Етапи атестування:

- визначення організації-виконавця атестування та оформлення відповідних організаційних документів;
- аналіз умов функціонування об'єктів інформаційної діяльності, технічної документації на комплекс технічного захисту інформації та розроблення й оформлення програми і методик атестування;
- здійснення випробувань відповідно до програми і методик атестування та оформлення протоколів випробувань і підсумкового документа – акта атестування.

Суб'єктами атестування можуть бути:

- Департамент спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України;
- організації-замовники атестування;
- організації-виконавці атестування.

До завдань Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України в цьому напрямі діяльності можна віднести:

- організацію розроблення та удосконалення нормативних документів з атестування;
- контроль виконання вимог щодо атестування та розгляд апеляцій;
- узгодження вибору організації-виконавця атестування, програм і методик атестування та результати атестування на особливо важливих об'єктах інформаційної діяльності.

Витрати на атестування зараховують до кошторису на проектування, будівництво та експлуатацію (утримання) об'єктів інформаційної діяльності. Організація-замовник на засадах, передбачених чинним законодавством щодо закупівель послуг за рахунок державних коштів, визначає організацію-виконавця атестування. Взаємини між організацією-замовником та організацією-виконавцем, яка є ліцензіатом, регламентує укладена між ними угода. У разі здійснення атестування на особливо важливих об'єктах інформаційної діяльності, визначення організації-виконавця атестування узгоджується з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України.

Організація-виконавець за результатами аналізу відомостей, наданих організацією-замовником, та, якщо є потреба, за результатами аналізу умов функціонування об'єктів інформаційної діяльності і загроз для інформації безпосередньо на об'єктах інформаційної діяльності, розробляє проект програм і методик атестування та подає його на узгодження організації-замовнику. Узгоджений організацією-замовником проект програм і методик атестування затверджує організація-виконавець. У разі атестування комплексу технічного захисту інформації на особливо важливих об'єктах інформаційної діяльності проект програм і методик атестування узгоджується також з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України.

Висновки. Обов'язковою умовою забезпечення захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності, є отримання об'єктивної оцінки рівня захищеності інформації, що здійснюється шляхом проведення державної експертизи та атестації.

Чинні в Україні нормативно-правові акти та нормативні документи недостатньо сприяють вирішенню проблем захисту інформації загалом та технічного захисту зокрема. Має місце проблема захисту персональних даних фізичних осіб та захисту відкритої інформації, спрямованого на реалізацію законних прав та інтересів особи, суспільства та держави.

Запроваджені останніми роками закони України щодо захисту інформації в інформаційно-телекомунікаційних системах, ліцензування, державного контролю господарської діяльності, підтвердження відповідності, метрологічного забезпечення діяльності, пов'язаної з вимірюванням фізичних величин, потребують вживання певних заходів з метою впорядкування системи технічного захисту інформації відповідно до вимог цих законів.

Усі ці чинники зумовлюють необхідність постійного розвитку всіх складових елементів системи технічного захисту інформації.

Література

1. **Karpinski M.** Elliptic Curve Parameters Generation / M. Karpinski, I. Vasylytsov, I. Yakymenko, A. Honcharyk // Proceedings of the International Conference TCSET'2004 "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (24-28 February 2004, Lviv-Slavsko, Ukraine). – Lviv : Publishing House of Lviv Polytechnic National University. – 2004. – PP. 294-295.
2. **Буров Є.** Комп'ютерні мережі / Є. Буров. – Львів : Вид-во "Бак", 1999. – 468 с.
3. **Домарев В.В.** Безопасность информационных технологий. Системный подход / В.В. Домарев. – К. : ООО "ТИД" ДС", 2004. – 992.

4. Кульгин М. Компьютерные сети: Практика построения: Для профессионалов / М. Кульгин. – М. : Вид-во "Питер", 2003. – 462 с.

5. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – Санкт-Петербург : Вид-во "Питер", 2003. – 318 с.

6. Фролов О. Система технічного захисту в Україні. Стан та перспективи розвитку / О. Фролов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2008. – Вип. 1(16). – С. 12-14.

Васильчак С.В., Байдак О.В. Порядок аттестации системы технической защиты информации

Все субъекты системы технической защиты информации, которые работают в сфере технической защиты информации, обязаны проходить соответствующую аттестацию. Проанализирован процесс аттестации системы технической защиты информации: этапы построения модели угроз информации, виды аттестации, порядок и сроки исполнения, определены объекты и субъекты аттестации.

Vasylchak S.V., Baidak O.V. Stages of a attestation the technical information security system

All subjects of the system of technical information security system, working in the field of technical protection of information must pass the appropriate attestation. Analyzed the process of a attestation the technical information security system: stages of building a model to deal with threats of information, apparently of attestation, stages of a process and timing for a regarding, determined objects and subjects of a attestation.

УДК 681.322.067

Доц. О.А. Нємкова, канд. фіз.-мат. наук –
Львівський ДІНТУ ім. В. Чорновола

ЗАВАДОСТІЙКЕ ПЕРЕДАВАННЯ СИГНАЛУ В УМОВАХ ШТУЧНО СТВОРЕНИХ ШУМІВ

Досліджено можливість завадостійкого передавання сигналу завдяки його спеціальній модуляції під час застосування інтегральних перетворень. Показано, що існує критерій, у разі виконання якого відновлюваність сигналу є задовільною. За допомогою комп'ютерного моделювання надано рекомендації з визначення параметрів модуляції, виходячи з характеру шумів.

Ключові слова: модуляція сигналу, шуми, інтегральне перетворення, завадостійкість.

Мобільний зв'язок сьогодні став невід'ємним атрибутом ділового суспільства. Вимоги до якості передавання інформації є дуже високими. Паралельно з розвитком якісного зв'язку спостерігається тенденція конструювання пристроїв, які не дають змогу проводити передачу шляхом створення штучних завад у місті локалізації передавача. В Інтернеті можна знайти багато пропозицій виробів, які блокують передачу мобільних телефонів, так званих глушників мобільних телефонів, які працюють у смузі робочих частот передавального пристрою. Робота подібних генераторів шуму не відчутна для людини, але робить мобільний зв'язок неможливим. Тому актуальним є розроблення завадостійкого передавання сигналів в умовах штучно створених завад.

Розглянемо можливість завадостійкого передавання сигналу завдяки його спеціальній модуляції під час застосування інтегральних перетворень. Пропонуємо таку схему [1]: у передавачі над дискретним сигналом $f(t)$ виконується інтегральне перетворення F (наприклад, швидке перетворення Фур'є), далі кож-