计算机电磁信息泄露分层防护策略的研究

余元辉

（集美大学计算机工程学院　福建　361021）

【摘　要】计算机系统工作时所发射的电磁波，有可能造成信息泄漏，会严重威胁到信息安全。本文首先以电磁学和天线理论为基础分析了电磁信息泄漏的机理，然后针对电磁信息泄露的过程提出了以“防辐射泄漏”、“防电磁截获”、“防电磁复现”的三层防护模型。最后从硬件防护以及软件防护两个方面，详细论述了计算机电磁信息泄露三层防护模型的具体实现手段。

【关键词】电磁信息泄漏；三层防护；防辐射泄漏；防电磁截获；防电磁复现

中图分类号：TP316.81　　文献标识码：A　　文章编号：1009-6833（2013）11-103-02

Research of the Layered Protection Strategy of Computer Electromagnetic Information Leakage

Yu Yuanhui

Abstract: The electromagnetic waves emitted by computer system at work, and may cause information leakage, will be a serious threat to information security. This paper first analyzed the mechanism of the electromagnetic information leakage based on electromagnetics and antenna theory, for the process of resulting in electromagnetic information leakage, “anti radiation leakage”, “preventing electromagnetic interception”, “and preventing electromagnetic emersion” is put forward. Finally, concrete implementation means of the three layers of protection model of computer electromagnetic information leakage is discussed in detail from two aspects of hardware and software protection.

Keywords: electromagnetic information leakage; three layers of protection; anti radiation leakage; preventing electromagnetic interception; preventing electromagnetic emersion

0　引言

随着信息技术的迅速发展，计算机已经广泛应用在安全机关、机要部门和银行金融等重要企事业单位。当计算机及其外设工作时，电磁波会通过传导或辐射的形式持续地向外发射，而这一过程常常和计算机的信息录入、信息传递、信息存储、信息处理、信息输出等环节紧密相连，发射的电磁波中往往“夹带”设备的有用信息，从而造成信息泄露。有相关研究资料表明，国外已研制出能在1000米以外的地方接收复现计算机电磁辐射信息的设备，敌对方完全可以利用这种方式隐蔽、及时、持续地获取情报[1]。特别是冷战后的一些西方发达国家，为了窃取他国重要军事情报不惜投入了大量的人力、物力和财力来发展电子窃听技术；而在现阶段，国内外一些犯罪团伙也企图通过不正当途径，采用高科技手段窃取国家或团体重要政治或商业机密[2]。因此，防计算机电磁信息泄漏已经刻不容缓，研究掌握有效的电磁信息泄漏防护措施尤为重要。

1　电磁信息泄漏的相关基础理论

由电磁学理论及实验可知，空间的运动电荷会形成空间的时变电流并产生时变电场，而时变电场又会产生时变磁场。二者相互关联，形成不可分割的时变电磁场。而麦克斯韦方程组正是用来描述电荷、电流与电磁场的关系，其基本形式被称为时域麦克斯韦方程，具体可分为积分形式和微分形式。其中积分形式如下：

$$\oint_l E\cdot dl=-\iint_s \frac{\partial B}{\partial t}\cdot dS \qquad (1)$$

$$\oint_l H\cdot dl=\iint_s \left(J+\frac{\partial D}{\partial t}\right)\cdot dS \qquad (2)$$

$$\oiint_s D\cdot dS=\iiint_V \rho dV \qquad (3)$$

$$\oiint_s B\cdot dS=0 \qquad (4)$$

微分形式如下：

$$\nabla\times E=-\frac{\partial B}{\partial t} \qquad (5)$$

$$\nabla\times H=J+\frac{\partial D}{\partial t} \qquad (6)$$

$$\nabla\cdot D=\rho \qquad (7)$$

$$\nabla\cdot B=0 \qquad (8)$$

上述公式中：

B——磁感应强度/磁通密度（Wb/ m^2）

E——电场强度（V/m）；

H——磁场强度（A/m）；

D——电位移矢量/电通密度（C/m^2）

J——电流密度（A/ m^2）

ρ——电荷密度（C/ m^3）

根据以上的麦克斯韦方程可知，由麦克斯韦方程可知电路中只要有随时间变化的电荷或电流，周围就会产生随时间变化的电场和磁场，这种时变的电场和磁场能互相转换，并具有波动性，且表现为电磁波的形式以一定的速度在空间传播，该过程也是能量的传播过程，即电磁辐射。

而根据天线理论，计算机中能够产生电磁辐射的部件（算机内部的各种传输线、信号处理电路、时钟电路、显示器、印刷电路板、开关电路等）都可以视为等效天线。除此之外，我们也不能忽视计算机的各种线路（地线、电话双绞线、电源线等），因为信号在这些线路中传输时会产生电磁能量的传导泄露。这些金属导体同样可视为等效天线。按照信息论的原理，辐射电磁波的等效天线可以看成通信系统中的信源，传播电磁波的自由空间可以看成为信道。如果在理想情况（即无噪声环境）下，计算机电磁辐射泄漏的电磁波信号均可以看成是电磁信息的编码。如果侦听者通过截获设备截获到泄漏的电磁波信号，就相当于获得了电磁信息的编码，进而就有可能复现出其中的有用信息。

2　三层防护模型

根据上述电磁信息泄漏的相关基础理论，计算机的电磁信息泄漏过程主要体现在三个环节：泄漏源（信源）、辐射泄漏的电磁波（信道）、截获设备（信宿）三个部分组成。在这三个不同环节上，计算机的电磁信息泄露表现出不同的特点，根据这些不同文章提出了一种以“防辐射泄漏”、“防电磁截获”、“防电磁复现”为目标的三层防护模型。首先，针对计算机的电磁泄漏，要采取措施尽量阻断或抑制计算机的电磁泄漏，使其泄漏出去的电磁辐射最少；其次，由于计算机的电磁泄漏不可能完全屏蔽，总会有部分电磁波泄露出去，所以要采用技术手段最大程度地增加截获设备获取计算机泄漏电磁波的难度，使其难于接收到；最后，如果截获设备有办法获得到计算机泄漏的电磁波，还应采用必要的方法尽可能增加对截获电磁波中所携带信息的复现难度。下图1为计算机电磁信息泄露的三层防护模型示意图。

图1中，计算机的三层防护策略模型中各层之间并非是孤立的。“防辐射泄漏”、“防电磁截获”、“防电磁复现”各层之间相互关联、相互补充。针对计算机不同部位的泄漏机理，三层防护策略的实现要综合考虑技术、成本、效果等因素，权衡利弊以便采取最有效的防护技术。

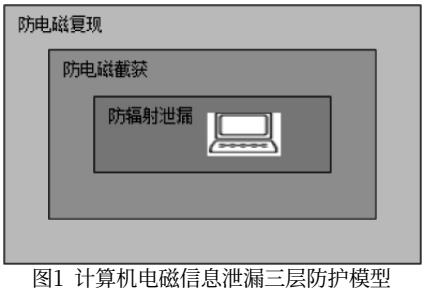


图1 计算机电磁信息泄漏三层防护模型

3 防护技术

通常可以采用硬件防护以及软件防护的技术，来实现计算机电磁信息泄露三层防护模型。目前基于硬件的计算机电磁信息泄露防护技术主要包括：使用低辐射设备、屏蔽技术、滤波技术、利用噪声干扰源、光纤传输技术。基于软件的主要包括：TEMPEST字体技术，RGB颜色配置技术，图像加噪技术等。

3.1基于硬件的防护技术

3.1.1使用低辐射设备

低辐射设备即TEMPEST设备，是防辐射泄露的重要措施。美国是研究防信息泄漏计算机（即TEMPEST计算机）技术最早的国家之一[3]。TEMPEST计算机正是采取防辐射技术设计和制造出来的，其目的就是尽量抑制计算机设备的电磁辐射泄露的限度，使其达到最低。比如显示器是造成计算机电磁信息泄露的一个重要外设，选用低辐射显示器就格外重要，而单色显示器的电磁辐射低于彩色显示器，等离子显示器和液晶显示器也能进一步降低辐射[4]。

3.1.2屏蔽技术

屏蔽技术往往是通过切断电磁波辐射的途径来抑制其空间传播，从而实现电磁信息泄漏防护的目标。其实质是是将计算机或计算机的关键电路、部件置于屏蔽室或法拉第屏蔽箱中，达到防止电磁辐射的目的。该技术是所有防辐射泄漏技术手段中最普遍采用也是最为可靠的一种。屏蔽室或屏蔽箱通常采用四种方法实现防计算机辐射泄漏的目的，这些方法包括：静电屏蔽、交变电场屏蔽、交变磁场屏蔽、交变电磁场屏蔽等,如美国研制的高性能的屏蔽室,其屏蔽效果对电场可达140db，对微波场可达120db，对磁场可达100db[1]。国内学者提出了高性能的电磁屏蔽方舱的设计要求，指出方舱设计时应注意几个部分：（1）选择屏蔽性能较好的铝板作为方舱壁板的内、外蒙皮，为了进一步提高屏蔽效能，壁板接缝处可采用高、低频性能都较好的镀锡铜胶带；（2）舱门设计时可加入电阻率小于0.01Ω·cm的环氧或硅脂导电胶；另外在界面处贴装导电屏蔽胶带；（3）通风口设计时要适当增加其厚度(孔的深度)，减小孔径，减小单个通风窗的面积，同时还确保通风口与舱壁的无缝导电连接；（4）空调过孔设计时采用铜管作为壁管，且铜管要采用特制的指型簧片紧贴方舱壁贯穿舱板；（5）转接口可采用导电插座并在插座与转接板间加装导电橡胶等导电衬垫[5]。

此外，屏蔽窗和屏蔽电缆也被经常采用。屏蔽窗主要指在计算机显示器上安装电磁屏蔽玻璃，它是通过在两层玻璃或透明树脂间夹经特殊处理的金属网压制而成的。电磁屏蔽玻璃可以将绝大部分的信息通过地线导入地下，只有极少的辐射漏网信号通过，即便侦听者有办法截获到这些信号也无法还原成清晰完整的信息，从而达到保密的目的。屏蔽电缆主要指在计算机电缆的外部加装屏蔽层，该屏蔽层可采用单层导线、双层导线或导线丝网和金属箔织成，它不仅能够提高电缆中信号的覆盖率，还能为电缆的传导辐射提供良好的屏蔽性。

3.1.3滤波技术

滤波技术是TEMPEST计算机技术中的重要内容。滤波技术主要是让位于屏蔽体内的计算机所辐射的在某些频率范围的电磁波，无法从屏蔽体内辐射出去而起到滤波作用，从而实现对计算机的电磁信息泄露防护。滤波技术一般采用滤波器来实现，滤波器按照用途可分为信号滤波器和电源滤波器，信号滤波器包括板上滤波器和连接器滤波器两种，滤波器的基本作用是选择信号和抑制干扰[6]。滤波器处理信号时会将其看成是模拟信号，并且该模拟信号是由不同频率的正弦波叠加而成。正是由于不同频率的正弦波存在，滤波器很容易通过选择不同的频率来实现信号滤波。目前，国内厂家制造的滤波器已能够大幅度地滤除计算机内PCB板上的各种线路所辐射的高次谐波，有效地防止计算机的电磁辐射泄露。

3.1.4利用噪声干扰源

利用噪声干扰源，其原理就是利用干扰器发射出来的电磁波去混合计算机辐射出来的电磁波，这样的“混合信号”令窃听设备很难截获到有用的计算机辐射信号，即便截获到“混合信号”也难于复现电磁波中所携带信息的内容、特征等。干扰器通常包括白噪声干扰器和相关干扰器。白噪声干扰器是干扰器早期产品，使用一台噪声发射器，在一个相对较宽的频带上制造很强的噪声，来覆盖计算机电磁辐射泄漏的信号；相关干扰器发出的干扰信号通常没有白噪声干扰器那么强烈，但往往与计算机电磁辐射信号相关，所以这样的干扰信号和计算机辐射出来的电磁波混合更能以假乱真。两种干扰器都可以提高侦听者对计算机电磁辐射信号的截获难度[7]。对于相关干扰器而言，即便侦听者有办法截获到电磁信号，但对信号数字处理也无法复现原来的信息，进一步提高了电磁信息泄漏的防护效果。通常干扰源被设置在计算机附近，这样干扰源与计算机所产生的电磁信息辐射一起向外辐射，使得计算机的辐射电磁波不易被截获和复现。我们国家已自主研发出专门解决计算机辐射泄密问题的相关干扰器，其型号为GRQ-03C。该款产品已经顺利获得中国人民解放军信息安全测评认证中心军B级认证，这也是目前国内军用信息安全产品认证的最高级别。它采用USB接口供电，无需外接电源，无需安装软件，兼容台式机和笔记本电脑，发射的干扰信号能够自动跟踪计算机显示模式的改变，自动适应各种不同模式下工作的显示终端，做到了时域上相同、频域上相关，抗视频接收还原能力强。

3.1.5光纤传输技术

光纤传输是主要的非导电介质传输技术。光纤通信中的光波主要是激光，激光具有高单色性、高方向性、高相干性等显著优点[8]。在使用光纤进行电波传输中，光信号会被完全限制在光纤里面，光纤的成分是玻璃纤维，玻璃纤维不会向外辐射电磁波，被截获的可能性几乎为零。由光纤周围环绕的都是不透明的塑料皮，即便出现电磁波泄露，其泄露的射线可能会被

塑料皮所吸收。因此，光纤传输技术具有非常高的防电磁信息泄露水平。探索频道宣称美国已于2012年11月1日成功研制了一种红外激光系统，并将其命名为“自由空间光学通讯”。该系统的示意图如下图2所示。这种激光通讯携带的信息量超过Wi-Fi等其他无线信号。由于红外激光束很窄，窃听者无法窃听和截获，除非他们正处在传输线路上。而窃听者一旦进入激光束的光束的传输线路，激光束将会中断并立即报警，因此系统具有较高的安全性。

图2 红外激光系统示意图

3.2基于软件的防护技术

3.2.1 TEMPEST字体技术

计算机显示器工作时会伴随着大量的数字/模拟信号转换，该过程所产生的高频频谱会包含大量的波峰，这些波峰可以被轻易地和噪声信号区分开来。窃听者往往利用高频频谱为线索去复现计算机的显示图像。所以，去除高频成分有利于提高电磁复现的难度，能够有效的防止计算机显示器的电磁信息辐射泄漏。英国的Kuhn and Anderson发明了一种称作Tempest字体的电磁信息防护方法，采用Tempest字体相当于低通滤波器、对计算机的图像或视频信号进行软件滤波，去除信号水平频谱当中顶端30%的部分，换言之减少了字体的高频能量，这种经过Tempest字体处理过的电磁波信号即便被截获，也无法复现泄漏信息的内容。并且TEMPEST字体技术比硬件防护技术更灵活且成本低廉，因此更有应用价值[9]。

3.2.2 RGB颜色配置技术

尽管触摸屏可以分为电阻式、电容式、红外线式、表面声波等不同种类，但其实现原理基本相似，都是将透明的触控面板叠加在普通液晶屏上。在实际生活中我们接触最多的还是电阻式触摸屏。这种触摸屏通常包括三部分：电极、两层透明的阻性导体层、两层导体之间的隔离层。触摸屏工作时，上下导体层相当于电阻网络。当某一层电极加有电压时，电压梯度就会在电阻网络上形成。如果此时手指触摸屏上某一点，屏幕上下两层便会在该处形成接触点，接触点处的电压可以通过电极未加电压的另一层很容易测得，进而获得接触点的位置坐标，该坐标信息通过接口（如RS-232串行口）传递给CPU，CPU就能判断出用户的输入信息，并将信息显示在液晶屏上。以电阻式触摸屏为例，在外力挤压触摸屏的过程中，因受压处各像素点压力发生改变，引起光线到达液晶时相应像素点的RGB分量电压差发生改变，在此过程中会出现电磁信号辐射，该辐射本质上是来源于液晶屏的光栅扫描过程中RGB信号模拟电压变化而发射的电磁波信号。如果窃听者设法截获到这些电磁辐射信号，就能利用图像分析重建技术复现出触摸屏显示的信息。

RGB颜色配置技术主要是通过优化配置触摸屏上按键的颜色，使得触摸屏上的按键在按下之前与按下之后的相对模拟电压差值保持恒定，即相邻像素RGB信号的模拟电压差值保持恒定。这样窃听者即便截获到按键操作所泄露的电磁辐射信号，也无法确定按键的状态从而隐藏了用户的输入信息，实现了此类由于触摸屏电磁噪声所带来的电磁辐射信息泄露。目前，RGB颜色配置技术已广泛应用于商业信息触摸屏设备上，如ATM、门禁控制终端、信用卡售票机等。

3.2.3图像加噪技术

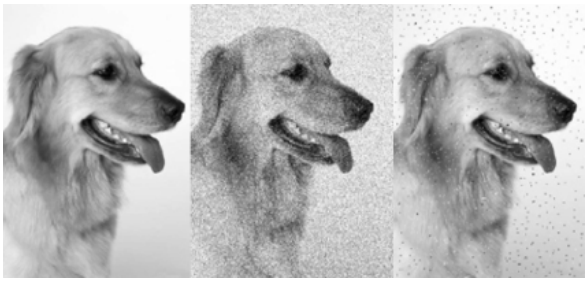
该技术通过在图像中添加噪声，在不影响视觉效果的基础上，实现防电磁信息泄露的目的。通常的图像加噪技术包括两种：一种是添加椒盐噪声，另一种是添加高斯噪声。

（1）添加椒盐噪声

椒盐噪声往往是由脉冲信号强度变化造成的，图像传感器，传输信道，解码处理等都会产生不同强度的脉冲信号，这些脉冲信号就会生成黑白相间的亮暗点噪声，从而随机改变图像中的部分像素值，影响了图像信息的表示，也可以说图像信息的表达更加复杂化。根据添加脉冲信号的强度不同，椒盐噪声通常分为两种：一种属于高灰度噪声，也叫盐噪声（salt noise），图像表现出来呈现白色杂点；另一种属于低灰度噪声，也叫胡椒噪声（pepper noise），图像表现出来呈现黑色杂点。而给计算机图像添加椒盐噪声时，往往两种噪声同时出现，图像呈现出来的效果就是黑白杂点。

（2）添加高斯噪声

高斯噪声是一种具有高斯分布（也称作正态分布）概率密度函数的随机噪声。或者说，高斯噪声在其各个频率分量上的能量具有高斯分布。在图像中加高斯噪声通常会使图像出现大量细小的斑点，使得图像变得比较模糊。图3显示了一幅图像在添加了椒盐噪声及高斯噪声后的效果。



(a) 原始图像　(b) 椒盐噪声效果　(c) 高斯噪声效果

图3 图像添加椒盐噪声及高斯噪声后的对比效果

4 结论

计算机信息处理过程中牵扯到大量的涉密信息，有的甚至关系到社会经济的稳定、国家的安全，一定要高度重视对计算机电磁信息泄漏的防护。文章所提出的计算机电磁信息泄露三层防护模型，就是要从“防辐射泄漏”、“防电磁截获”、“防电磁复现”三方面统筹考虑计算机系统的电磁防护，从而提高计算机系统的信息安全。当然，计算机防电磁信息泄漏是非常复杂的系统工程，光有抽象的防护模型是远远不够的，还要将模型与具体的计算机系统结合起来，并采取相应的软、硬件电磁防护措施进行综合防护，才能实现最佳的电磁防护效果。

参考文献：

[1]赵立华,刘容平.计算机的电磁泄漏及防护技术[J].信息网络安全，2002.

[2]樊文琪.信息设备电磁泄漏发射与防护[J].电子产品可靠性与环境试验，2005.

[3]吕立波. 基于电磁泄漏的信息安全研究 [J]. 办公自动化，2007.

[4]李务斌,张志华,戴冬原 .低辐射加固液晶显示器设计[J]. 电子机械工程，2012.

[5]朱静.方舱的电磁屏蔽设[J]. 现代电子工程，2004.

[6]屈耀红,闫建国,卢京潮 . 某型无人机GPS／Radio／DR组合导航中的滤波技术研究[J]. 系统工程与电子技术，2004.

[7]夏志军,肖继刚,王肖,章新华,许林周,范文涛. 噪声干扰器对抗主动声纳有效干扰压制区计算方法[J]. 系统工程与电子技术，2012.（下转99页）

2.2 进行信息化建设统一规划

应通过加大企业网络与自动化建设，不断夯实基础，进一步扩展企业的网络和通信覆盖面，同时，在企业员工中积极开展信息基础知识教育培训。通过提高资源整合、加强有效管理和进行技术标准化等措施，加强企业信息化平台建设，认清信息化建设形势，转变观念，建立统一、全面、高效的网络平台。各专业业务系统开发前，应从基层单位征求意见或进行实地调研，明确需求，使各专业系统在使用中更“接地气”，减少运行后修改维护工作量，避免一些后期发现且无法解决的软件“硬伤”。在数据共享方面，在企业内部应加强控制，使各部门、单位能共有效共享各类资源，降低企业运营成本，实现利润最大化。

2.3加强局域网络管理与维护

供电企业信息化是通过网络组建实现的，目前供电企业内部的局域网已建成，加强网络日常管理与维护成为信息化建设的一项重要工作。局域网之间的信息传输主要是通过网络拓扑结构来实现的。其中拓扑结构有环形拓扑结构、树形拓扑结构和星型拓扑结构等，他们之间可以互相组合，进而组成局域网运行的基础构架。局域网的硬件主要包括工作站、网络服务器、路由器、网桥、网管、网络传输中的线路。根据拓扑结构和连接线路的不同，还需要集中器和集线器等特殊设备，以满足特定应用要求的网络软件的正常运行。对这些设备的维护是保证信息化建设水平的基本要求。对服务器、交换机、路由器、配线架、网线等设备，每年至少进行一次进行全面检查和预防性维修，更换一次性能波动或超过使用寿命的设备及部件。在网络出现异常征兆或故障情况下，进行应急维修，检查、分析、确定故障设备或故障部位，排除故障。

2.4 及时进行系统备份，提高网络容灾能力

在做好网络安全管理工作的同时，也应考虑系统在不可避免的因素下出现的故障恢复需要。为保证网络设备出现突发故障时，能够及时恢复数据，要定期对重要设备、重要数据进行备份。一般数据恢复分为对硬件进行恢复和对软件进行恢复。对重要数据的存储和重要软件的运行设备应准备一套硬件备份。硬件恢复可使用硬件替代、固件修复、数据读取等方法。根据供电企业信息化员工业务水平，硬件替代可自行解决，固件修复和数据读取一般要依靠技术可靠、安全保密性强的专业单位进行处理。软件恢复包括系统恢复和文件恢复。在操作系统和应用软件不能正常启动时，可使用修复软件进行修复，现在的普遍做法是利用ghost、livestate对系统进行全盘备份，可以快速恢复系统正常工作。文件恢复则是存储介质上的应用文件损坏，可用修复软件进行修复，从而恢复文件数据。目前文件修复软件种类很多，可根据需要进行选择使用。

2.5 加强网络备用通道建设

随着供电企业信息化建设的不断深入，网络运行可靠性越来越影响各业务系统的使用，现在，应逐步加强对备用通信通道的建设。通过敷设备用光缆、无线通道或与移动、电信等企业合作建立应急网络通信渠道，在现有网络出现故障时，及时启用，保障各项业务系统使用和日常业务的正常开展。

2.6 强化信息化建设安全保障工作

信息化建设的安全问题关系到企业的信息安全和长久发展，也是决定供电企业信息化建设的关键因素。局域网信息安全面临着UDP 攻击、网络即时通信窃听、ARP 欺骗、密码嗅探、邮件窃听、基于TCP 的攻击等威胁，为提高网络安全性能，要从安全保障体系、信息安全框架、安全管理、认证和加密技术以及安全标准化等方面入手，解决信息化建设的安全问题，为企业的信息化管理提供基本保障。不断完善有关安全法律和规范，尽量减少人为破坏、误操作等行为的出现。要设立专门人员负责专门的信息输入、储蓄和发布，完善内外网系统的隔离和重要文件的储备工作。

在技术层面，可以采取通信加密、网络分段、划分VLAN、入侵检测，漏洞扫描、安装防火墙和杀毒软件等防范措施。除了在技术方面采取一些措施外，更要加强管理。没有完善的管理，网络安全防范只是空谈。即使企业配备了最先进昂贵的信息安全设备，但管理“政策”或“人”不配合，仍旧会产生很大问题。即使安全防护设置了层层关卡，仍可能因为密码被破解、临时开放的权限未及时关闭、网络文件夹被轻易共享等管理盲点，为黑客及病毒开启后门。因此，信息安全是管理问题，而非单纯的技术问题。安全管理是一个动态管理的过程，会随着时间的推移和业务的发展而变化。在管理层面，应从提升组织的整体安全意识、对重要目标进行安全训练、建立必要的运作规程、构建安全环境，加强信息安全技术平台的建设、加强企业内部的安全技术建设和监管工作、加强员工实施安全培训，提高员工个人的安全意识等方面入手，提高信息化建设的安全性能。

2.7 培养信息化人才

供电企业应通过平等待遇、增强激励等方式培养一批高效的、专业的信息化建设人才。把信息化建设和业务管理放在同等的地位对待，在日常工作中，积极开展信息化专业人员培训、岗位练兵、专业竞赛等活动，为从事信息岗位员工提供发展空间和施展才能的平台，加强信息化人才储备，提高信息化人才在供电企业中的地位。加强企业其他员工信息化知识培训学习，营造良好的学习氛围，提高企业整体信息化应用水平。进一步培养复合型的人才，特别是在管理层要培养一批既懂业务管理又懂信息技术的管理人员，这样在管理上才能进一步提高水平。建立和完善供电企业信息化方面的人才管理和评价机制，采取合理有效的激励和绩效考核手段，调动员工积极性，不断完善用人制度，通过竞争、择优上岗，优化人力资源配置。

2.8 探索电量电费等数据在互联网开放查询

在互联网应用全面普及的今天，广大客户在互联网上进行个人用电信息查询的需求越来越迫切，目前供电企业已实现网络缴费功能，但用电信息查询尚未实现，该项业务的开通，需要信息化技术的大力支持，考虑到信息量大及网络安全等因素，这项业务还需要进行周密的设计、稳步推进和积极探索，争取早日实现，满足客户需求。

参考文献：

[1]薛华成.管理信息系统[D].北京:清华大学出版社,2003.
[2]方刚等 局域网信息安全面临的威胁分析和防范措施探讨 网络安全，2007
[3]王志宏等.管理信息系统在电力企业管理中的作用[J]. 辽宁工程技术大学学报(自然科学版),2001(2).
[4]杨振宇等。浅析计算机软件可靠性设计 中国新技术新产品 2011

（接上105页）

[8]何林飞,田佳月,张晓林. 基于光纤传输的多路高速数据采集系统[J]. 电子技术应用，2013.
[9]袁祁刚,国伟. 军用电子设备电磁信息防护技术[J]. 装备环境工程，2006.

作者简介：
余元辉(1973-)，男，硕士，副教授，硕士研究生导师，研究方向为信息安全，人工智能等。

基金项目：福建省科技厅资助省属高校专项基金项目(JK2012026)