网络时代高校信息安全体系建设研究

WANGLUO SHIDAI GAOXIAO XINXI ANQUAN TIXI JIANSHE YANJIU

张丽华◎著

中国水利水电出版社
www.waterpub.com.cn

网络时代高校信息安全体系建设研究

张丽华◎著

中国水利水电出版社
www.waterpub.com.cn
·北京·

内 容 提 要

随着我国信息化建设的日益推进，国民经济和社会发展对网络和信息系统的依赖越来越紧密，尤其是高校的信息系统已经成为重要基础设施，这些信息系统的安全运行直接关系到师生的利益和社会的稳定。

本书对网络时代高校信息安全体系建设进行了研究，主要内容包括相关理论综述、网络时代高校信息安全现状、网络时代高校信息安全面临问题原因分析等。

本书结构合理，条理清晰，内容丰富新颖，具有较强的可读性，可供信息安全领域的工程技术人员参考使用。

图书在版编目(CIP)数据

网络时代高校信息安全体系建设研究 / 张丽华著.
—北京：中国水利水电出版社，2018.4
ISBN 978-7-5170-6427-5

Ⅰ. ①网… Ⅱ. ①张… Ⅲ. ①高等学校－信息安全－研究 Ⅳ. ①G647

中国版本图书馆 CIP 数据核字(2018)第 092492 号

书　名	网络时代高校信息安全体系建设研究 WANGLUO SHIDAI GAOXIAO XINXI ANQUAN TIXI JIANSHE YANJIU
作　者	张丽华　著
出版发行	中国水利水电出版社 (北京市海淀区玉渊潭南路 1 号 D 座 100038) 网址：www. waterpub. com. cn E-mail：sales@waterpub. com. cn 电话：(010)68367658(营销中心)
经　售	北京科水图书销售中心(零售) 电话：(010)88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京亚吉飞数码科技有限公司
印　刷	北京一鑫印务有限责任公司
规　格	184mm×260mm　16 开本　12.25 印张　298 千字
版　次	2018 年 6 月第 1 版　2018 年 6 月第 1 次印刷
印　数	0001—2000 册
定　价	57.00 元

前　言

信息安全问题是当前世界范围内各种机构组织亟待解决的问题之一。与以往只关注信息安全的技术研究不同，信息安全问题实际上包括技术、管理和法律在内的系统工程，高校人员密集，信息安全是校园治安防控体系的重要组成部分，切实筑牢校园安全屏障，确保高校安全形势持续稳定。

人类在信息的海洋中生存和发展，正是通过信息来区别不同事物、认识不同事物和改造世界的。信息安全，尤其是高校的信息安全，一直是广大师生都十分关注的话题。当前，虽然我国出台了一些相关政策和管理办法，据专家分析，由于专职的安全监管机构的缺失，使得信息系统安全工作很难落实。近些年来，国内外发生的一系列事件表明，如果重要信息系统没有一定的安全防范能力，一旦发生重大事故或遭遇突发事件，将会造成不可挽回的经济损失。我国相关部门对信息安全工作十分重视，国务院信息化工作办公室司长王渝次曾指出，灾难恢复是信息安全保障重要的基础性工作，做好国家重要信息系统灾难恢复工作，提高其抵御灾难和重大事故的能力，对于确保重要信息系统数据安全和业务的连续性，保障社会经济的稳定是非常重要的。2003 年颁发的《国家信息化领导小组关于加强信息安全保障工作的意见》，对重要信息系统的安全做出了明确要求。2004 年，国务院信息办又组织起草了《重要信息系统灾难恢复指南》，并印发给各基础信息网络和重要信息系统主管部门。然而，高校的信息化虽然取得了快速发展，但其背后隐藏着可怕的问题：虽然在实现了数据大集中的高校中有 80%的高校做了系统灾难备份中心的建设，但真正能实现业务连续管理的，估计只有 15%左右。最近，高校系统故障不断，出现了安全事故，校方还不知道有黑客造访。邮箱系统无法正常使用、教务系统中的文件不能正常下载等，这一切为校园信息安全敲响了警钟。

随着高校顺应趋势的开放和互联，其信息安全范畴已经突破了以业务系统物理隔离和协议隔离为基础的传统信息安全。我们必须在一个日趋开放的系统平台上重新审视高校的信息安全问题。高校是国家政策要求实施安全等级保护的关键信息基础设施的重点系统。因此，如何建立一个高效的现代信息安全体系，日益成为突出的问题。本书从国内外有关信息安全管理的现实情况出发，论述了加强高校信息安全管理的重要性；研究了信息安全的基本理论；从高校实际情况出发，分析目前信息安全的现状、面临问题的原因分析，提出不仅需要从管理角度加强法律法规建设、健全管理体系、提高师生的安全意识上下工夫，并且从技术角度给出了高校信息安全防护的应用方案，最后对研究工作做了简要的总结，并提出了进一步研究的设想。

目　录

第1章 绪 论

1.1 背景与意义

1.1.1 研究背景

从互联网诞生以来，中国人的信息安全意识就很淡薄，要说重视，只限于军事、政治方面，因为这关系到一个国家的核心机密和情报。其他领域没有任何防范设施、没有禁区，窃取信息就像在没有上锁的房间拿东西一样方便。网络环境下我国信息安全状况更是堪忧。我国信息安全在管理和技术方面起步晚，因而没有形成完善的管理体系，在技术上比较落后。但近几年来面对国际信息环境的变化与挑战，我国也采取了一系列对策。2004 年 1 月，在北京召开了“国家信息安全保障工作会议”，会议强调了信息安全的重要性；2005 年，党的十六届四中全会将信息安全提升到一个新高度，它的地位等同于政治安全、经济安全、文化安全，这在党的历史上是前所未有的；科技部制定的“十一五”国家科技支撑计划发展纲要中明确指出：“十一五”期间的发展目标定位于突破核心技术，初步建立具有中国特色的信息安全保障体系。2006 年《2006—2020 年国家信息化发展战略》将建设国家信息安全保障体系列入了我国信息化发展的战略重点，并制定了一系列与信息化有关的法律法规，主要有：《计算机病毒防治管理办法》《计算机信息系统安全保护条例》《计算机软件保护条例》。

2014 年 2 月，中央成立网络安全和信息化领导小组，习近平主席担任组长，其在中央网信领导小组第一次会议上提出“没有网络安全就没有国家安全”。所有一切已经说明：在我国信息安全已经上升至国家战略高度。国家对信息安全的重视程度日益提高，很有可能在政策落地后，对国产软件研发方面投入更多的资金和技术上的支持。

在高校实行信息安全责任制是教育部的工作重点。2015 年 2 月，教育部办公厅印发了《2015 年教育信息化工作要点》，工作要点指出：本年度加强信息技术安全的重点放在部直属机关、部属高校，安全责任制度必须得到彻底的贯彻执行，工作机制进一步完善。信息系统安全等级保护工作必须在公安部指导下部署，网络安全通报机制在各部属单位落实，安全事件实时监测机制、安全事件应急预案在每个单位得到有效落实。

目前，高校是我国信息化建设的重要基地，大部分高校的信息化建设均已完成。现如今高校的校园网已经成为教职员工进行教学、科研、管理及学生日常学习生活不可缺少的重要组成部分。随着网络技术在高校工作中的普及，一方面需要为广大师生提供海量的信息资源、多样的娱乐方式以及丰富的服务形式。同时，网络本身存在的安全隐患以及由此带来的一些变化

使得其原有的信息安全防范措施不能保障高校的信息安全。从我国高校目前的信息安全现状来看，不管是软硬件系统、组织结构还是信息管理方面，均有不同程度的安全隐患存在。数据丢失、系统宕机、业务停顿、网络中断等经常发生，这属于信息安全事故的范畴，所有迹象说明我们的技术水平落后，在内部管理上存在漏洞，信息安全监管上缺失，个人信息安全意识没有得到很好的加强。

本书在互联网大环境下，从技术、管理视角两个方面去解析高校的信息安全保障体系，目标是所建立的信息安全保障体系可以应对互联网环境下各种信息安全挑战，所做的研究一方面让信息安全管理的有关理论得到完善，另一方面在日趋复杂的互联网环境下对信息安全保障的概念、构成等有更进一步的诠释；对于在互联网环境下，更好地建设高校信息安全保障体系等现实问题提供一个新的思路。

1.1.2 研究意义

矛和盾是相互对立的、又是统一的，事物发展的源泉来自于矛盾。信息安全和不同种类的安全威胁构成了矛盾体，矛和盾两者在彼此促进中共同进步。我们现在所处的信息社会是开放的、包容的，最初建立互联网的时候，没有考虑安全因素，由此所带来的后果是各种风险和威胁随处可见。由此看出，一方面我们在享受着信息化给我们带来的方便，另一方面我们必须持续地研究信息安全的特点，提出面对不同威胁我们所要采取的解决信息安全问题的各种办法。随着以信息技术为核心的各种新技术的快速发展，不仅缩小了国与国之间的距离，而且形成了地球村。2001 年中国加入了世贸组织，高校面临的形势更加严峻。知识经济时代数字化、网络化的发展对高校提出了更高的要求，我国高校为了生存和发展必将加快以高技术手段为基础的科技创新，这对计算机安全信息管理提出了新的挑战。

2016 年，“十三五”进入第一个年头，建设更符合其业务特性和应用系统现状的 IT 架构，改变过去那种作坊式信息系统应用建设方式，强化规划指导作用，整体协调推进科技和业务的发展，将成为高校信息化“十三五”规划和建设的主旋律。高校信息系统的安全关系到教育系统的安全稳定，关系到国民经济持续发展和国家安定团结，它的安全问题如果解决不好，将使国家教育处于危险之中。根据高校信息安全现状和发展需要，对高校进行实证研究和理论研究，提出一套切实可行的管理制度和方法，指导高校理清信息安全工作思路，尽快建立起有效的高校信息安全管理的工作方法体系、规章制度体系、技术防范和监控体系，对提高高校防范信息入侵和攻击能力，及时有效地抑制和打击计算机犯罪，保障高校安全运行，降低和化解风险，对促进国民经济的顺利发展和保持社会稳定具有重要意义。信息安全管理得到关注、完善，势必使得高校面向社会提供的服务更上一层楼，这是高校可持续发展必经之路。

信息安全不是简单地把各种产品安装上，不是简单的排列，是不间断地监督、审核、调整的动态维护过程。在整个信息安全防护过程中，人是最主要的因素，然后才是技术、操作。三者需要有机地结合起来。

现代社会将信息、材料、能源列为三大资源。信息资源分布在社会的方方面面，它拥有与众不同的特征：多效用性、压缩性、共享性、增值性、扩充性、普遍性和可处理性，因而信息资源对于人类社会具有特别的意义。信息安全的内涵是对信息系统、信息资源实施保护，使它们不再遭受各种威胁、破坏、干扰，也就是让信息处于安全状态之中。

信息安全上升到国家层面是战略问题。对于高校来说，信息安全影响到正常运转和可持续发展。高校的校园网中涉及人事、财务、招生、迎新、教务、一卡通等多种应用系统，这些信息资源一旦受到攻击或者破坏，造成的损失无法估量。由此看来，信息安全是高校得以健康发展的重要前提，不重视信息安全，终将造成高校处于危险之中。总而言之，信息安全的建设要着眼于全局，而不能仅限于局部，同时，信息安全建设是一个可持续的、发展的、动态的管理过程，而不是技术过程。

1.2 国内外研究现状

1.2.1 国外研究现状

21世纪是人类迈步走入信息化的时代，国与国之间的斗争不再是武力争霸，取而代之的是网络控制、渗透。先进的信息技术可以达到不战而屈人之兵的效果。一个国家如果不能掌控自己的信息安全，那么从何而谈国家安全呢？

目前信息安全的国际大环境发生了不小的变化：计算机用户数量越来越多，互联网普及率在提高，信息空间已经变成经济、政治、组织、社会和战争的运营环境而出现，数字融合使信息以不同形式和方式组合、改变和再利用，全球互联让计算机系统操控全面的基础设施。国家、组织、个人身处在信息环境之中，每时每刻通过互联网实现互相交流的目的。互联网的兴起带动了一大批产业的发展，比如：网上购物、电子银行、电子商务、电子税务等，所有这一切正深刻地改变着人们的生产生活、消费方式。

与此同时，国际上的信息安全事件层出不穷。2016年6月路透社曾经报道，来自于美联储的网络安全记录中记载了2011—2015年5年间，针对自身计算机系统的网络入侵高达50多次，被美联储工作人员描述为“间谍活动”的就有好几次。美国马里兰大学校长华莱士·D·罗于2014年2月19日发布了一个重要声明：在一次电脑安全攻击中，学校的数据库发生了重大泄露，事件发生的时间在2月18日。长期以来由学校信息技术部维护这一数据库，数据库中存储着大量个人数据，主要有1998年以来将近31万名学生、教职员工的信息。这些信息包含社会安全号码、姓名、生日和校园识别码。这些信息如果泄露出去对生活造成的影响不可预测，因为有了姓名、社会安全号码和生日，别有用心的人就可以用这些信息开设假帐户、盗取个人信用等。2015年12月23日，乌克兰电网遭到恶意攻击，攻击的后果是伊万诺—弗兰科夫斯克州变电站总控系统被破坏，后经调查获知：停电是由黑客袭击造成的，使用的恶意程序是Black Energy。2016年11月，英国最大的移动运营商——Three公司，黑客用员工帐号登录到数据库，该数据

库约有 600 万用户的相关信息。美国金融时报报道，国际上计算机安全事件发生的频率为：平均每 20 秒发生一起。

一系列信息安全事件发生后，一些发达国家，特别是信息化程度比较高的国家，对信息安全给予高度重视。作为互联网的发源地和世界首屈一指的信息强国——美国，对信息安全重视程度越来越高，在一些比较有名高校专门设立了信息安全管理部门。例如斯坦福大学设有信息安全办公室(Information Security Office，ISO)，印第安纳大学设立了信息技术安全办公室(Information Technology Security Office，ITSO)。与此同时，大部分欧洲的高校建立了比较成熟的信息安全管理体系。

目前，国外高校校园网的基础设施建设和信息安全管理方面都比我们国家更完善，为在校师生提供了安全、稳定、高效的校园网络服务。他们不仅有国家层面的网络安全标准及信息技术作支撑，而且在信息安全体系建设上经验丰富。

1.2.2 国内建设现状

中国的信息化开始得晚些，信息技术前进的步伐慢些，因而所发生的信息安全事件没有那么多，尽管如此，信息安全工作必须引起高度重视。不论在信息安全的技术上，还是在信息安全的意识上，我国目前都相对滞后，日益严峻的信息安全问题摆在我们面前。1998 年 4 月，华南一所大学的学生，在《羊城晚报》上发表了一篇文章，文章内容中含有大量国防科研信息，事后调查得知：这名学生就读的学校网站上转载有大量涉及军事重要机密信息的文章。1998 年 9 月的一天，郝氏两兄弟把遥控发射装置安放在工商银行储蓄所，利用高科技侵入银行的 IT 系统，非法盗走了 26 万元。第十五次全国信息网络安全状况调查结果显示，2015 年，64.22% 的被调查单位发生过信息安全事件；63.89% 的计算机感染过病毒，相比 2014 年增长了 0.19%。

当然，随着国际上信息安全不断发展，我国的信息安全标准体系也在建设中。如今，国家信息安全组织保障体系在我国已初显规模：国务院信息办牵头，网络与信息安全领导小组建立起来，分支管理机构在各省、市相继建立。2001 年 5 月，我国成立了中国信息安全产品测评认证中心，从此以后，信息安全测评认证工作就由它开展，代表国家形象，遵照国家有关信息安全管理的法律法规、产品质量认证来进行，国家信息安全的一切事务由中国信息安全产品测评认证中心全权负责。同时，信息安全测评认证体系也随之建立。2003 年 7 月国务院信息化领导小组通过并开始实行《关于加强信息安全保障工作的意见》，9 月，中央办公厅、国务院办公厅下发了关于加强信息安全保障工作的意见，该意见的指导方针是“积极防御，综合防范”，并且要求把信息安全工作视为与维护社会稳定、促进经济发展以及保障国家安全这类同等重要的工作来抓。除此以外，我国还制定了一连串信息安全管理标准，属于国家技术标准的有《信息系统安全等级保护基本要求》《计算机信息系统安全保护等级划分准则》(GB 17895—1999)；属于管理规范的有《信息安全技术信息系统安全管理要求》(GB/T 20269—2006)、《信息安全技术信息系统安全工程管理要求》(GB/T 20282—2006)、《信息系统安全等级保护基本要求》等；引进了国际上著名的信息安全管理标准：BS 7799—2：2000《信息安全管理体系实施规范》、ISO 17799：2000《信息安全管理实施准则》等。当然，仅仅是

标准方面的建立是不够的，我国还制定了一系列与之对应的信息安全管理法律和法规。自20世纪90年代以来，信息安全的管理工作需要社会各方面的协调配合，我国多方联合共同制定了关于信息安全管理的法律法规文件，主要包括：《计算机信息网络国际联网安全保护管理办法》《电子签名法》《中华人民共和国计算机信息网络国际联网管理暂行规定》《互联网信息服务管理办法》《商用密码管理条例》等。信息安全管理不仅需要标准、法律、法规的实施，而且信息安全风险评估工作也是重要一环，信息安全核心工作就是风险评估。对我国核心城市的10多个行业，涉及50多个单位，由国家信息中心带头组织展开相关调查研究，其调查研究的结果是产生了一批相当有影响力的报告，比如《关于加强信息安全风险评估工作的建议》《信息安全风险评估研究报告》《信息安全风险评估调查报告》等，通过这次调研，获取了大量的第一手实践资料，最终制定了《信息安全技术信息安全风险评估规范》(GB/T 20984—2007)。

近年来，随着国家信息化建设的快速发展，国内在高校信息化建设和管理方面的研究不断深入，高校信息安全方面的研究有所涉及。

硕士论文《网络环境下高校图书馆信息安全保障体系研究》是由安玉杰撰写的，该文在论述图书馆信息安全管理现状的基础上，阐述了现今图书馆在信息安全管理方面存在的不足，接着为图书馆量身订制了一套息安全保障体系。文章目的在于：建设一个全新的信息安全保障体系，在新形势下高效地保护图书馆信息资产的安全，让它能够连续运行。从论文题目可看出，研究仅面向高校的图书馆，不完全适用于高校信息安全管理。寻求适合整个高校的信息安全体系，则需要更全面的制度、机制和办法等。

我国学者在信息安全领域也做了很多研究。罗力(2012)解析了信息安全和信息安全素养的内涵，信息安全素养包含的内容比较广泛，主要有信息伦理道德、信息安全能力、信息安全知识、信息安全意识等，在信息素养的体系中占据核心地位的是信息安全素养。最后构建了公民信息安全素养评价指标体系，所依据的是信息安全素养的内涵，采用的是过程——目标结构法。

梅生伟等(2011)从复杂网络的视角对智能电网信息安全做了相关评述，认为信息安全对智能电网全系统存活性的影响在理论和工程两方面均具有重要意义。杜勇等(2010)论述了电子商务信息安全工作应有的特征及其对从业人员的素质要求，运用各种模型确定评价等级及权重，最后创建了综合评价矩阵，面向目标人群是电子商务信息安全人员，辅助企业选择更加适合岗位需求的优秀人员。胡勇等(2008)在信息安全方案中，首先针对对抗风险的效能指数进行计算，接着针对全体影响因素的权重赋值，再计算信息安全方案综合指数，最后对信息安全方案进行排序，按照综合指数来排序，最终实现对信息安全方案做出最恰当的抉择。李天目等(2007)文中用多任务委托——代理模型作为原型，从两个方面即信息安全绩效评估和技术工作的效果测评。测试了信息安全的激励效果，最后利用三角函数展示两者间的联系。

综上所述，我国对信息安全的研究，多数关注的是技术层面，重视管理的，也都是泛泛而谈，可以将技术、管理有机结合，制定一套在实际中可行、操作性强的研究成果不是太多。

1.3 研究内容和方法

1.3.1 框架结构

本书以信息安全体系建设为中心，对高校展开研究，总结了高校信息安全体系建设的经验，分析存在的信息安全问题、成因，并探讨新的思路和举措，力求将相关经验推广至其他高校。

1.3.2 研究内容及技术路线

(1)信息安全概述

介绍了信息和信息安全，信息安全需求，信息安全技术等方面的内容，进一步分析信息安全管理及对信息安全的正确认识。

(2)高校信息安全面临的挑战

主要从来自信息流动途径的挑战，校园网信息安全技术不成熟，信息安全管理体制不完善，信息安全法律法规不健全等方面分析高校信息安全所面临的挑战。

(3)高校信息安全面临挑战原因分析

按照前面提出的挑战来分析原因，主要从这几方面进行分析：信息安全管理缺乏协调，信息安全值得担忧，高校师生信息安全意识普遍淡漠、立法不健全，基础信息产业严重依赖国外，全球信息化对高校信息安全的冲击。

(4)高校信息安全保障体系建设

针对以上问题，提出具体措施：加强校园网信息安全法律法规建设，完善校园网安全技术保障体系，健全校园网信息安全管理体系，提高师生的信息安全意识。

本书的技术路线如图 1-1 所示。

1.3.3 研究方法

要想探究一个问题，一定要采用科学的研究方法，利用相关工具进行深入的研究，否则就是对问题的表面泛泛而谈，不可能深入其中，更不会透过现象看清本质，找到问题的规律、逻辑关系，因而研究方法至关重要，决定你的研究过程、结论是否科学。本书也力图使相关的分析过程和结论建立在科学的研究方法基础之上，寻找出信息和校园安全的内在逻辑关系，以对信息与校园安全之间的关系有一个比较清晰的解读。因此，本书将采用：

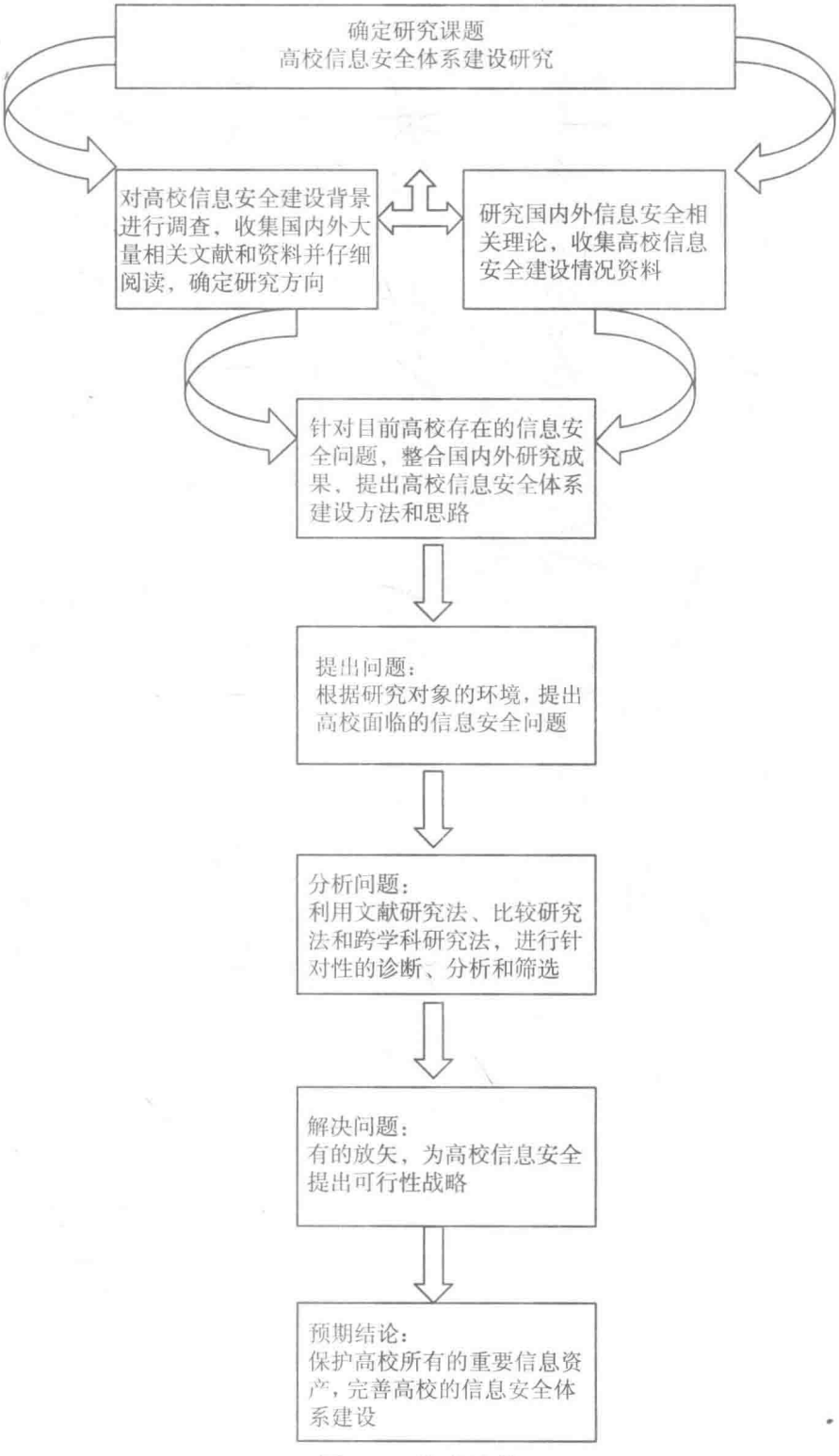
确定研究课题
高校信息安全体系建设研究
对高校信息安全建设背景进行调查，收集国内外大量相关文献和资料并仔细阅读，确定研究方向
研究国内外信息安全相关理论，收集高校信息安全建设情况资料
针对目前高校存在的信息安全问题，整合国内外研究成果，提出高校信息安全体系建设方法和思路
提出问题：
根据研究对象的环境，提出高校面临的信息安全问题
分析问题：
利用文献研究法、比较研究法和跨学科研究法，进行针对性的诊断、分析和筛选
解决问题：
有的放矢，为高校信息安全提出可行性战略
预期结论：
保护高校所有的重要信息资产，完善高校的信息安全体系建设

图 1-1　技术路线

(1)文献研究法

研究问题时,先要搜集大量的文献资料,然后有鉴别地整理、分析搜集到的文献资料,只有这样才能全面准确掌握该研究的前沿技术、研究方法等。本书在选题、写作的过程中大量阅读研究了国内外的相关文献资料,并通过深入挖掘和综合分析来确立了论文选题、框架和主要内容,同时也通过对相关文献的综合分析来寻求可能的创新与突破。

(2)比较研究法

在当前全面走向信息化的国际态势下,比较、分析不同行业对信息安全的认知和行为,找出其中的一般规律,并力求制定出符合信息化时代客观规律的信息安全政策。

(3)跨学科研究法

由于信息的概念非常之广泛,而信息安全之概念也在不断扩大之中,因此,本文将不囿于高校的信息安全,而是综合银行、企业等多行业的信息安全方面的知识,进行系统化的研究。

1.3.4 创新点

本书的创新之处主要有以下几点。

(1)主题新颖

本书在互联网的大背景下,研究高校信息安全体系建设。信息安全在金融业已经有了很多研究成果,但是信息安全和高校相结合的研究却寥寥无几,然而高校的信息安全体系建设具有极大的现实价值。

(2)机构和制度建设创新

网络时代高校信息安全管理体系不仅需要制度建设,而且还需要校内众多部门的协调配合,本文首次提出成立信息安全领导小组(校级)作为权威机构;率先制定了高校的信息安全管理制度。

(3)备份策略的创新

首次提出了除了采取热备份外还应由教育主管部门统一对高校实现异地容灾备份,这样可以抵御大规模天灾人祸。

第 2 章　相关理论综述

在信息安全研究领域，有业内公认的信息相关理论，我们对其进行总结分析，为本书的撰写提供了丰富的理论基础和素材，在本章对部分理论研究成果进行了归纳和整理。

2.1　信息和信息安全

伴随着中国经济的快速发展，我国信息化的步伐有了明显的进步，截止到目前，无论是行政机关、各大金融机构、企业事业单位、国企、私企，都离不开 IT 系统，信息技术已经深入到政治、经济、文化、社会生活的各个角落。我们是那么的依赖 IT 系统，所以 IT 系统中的信息、服务二者的安全是不容忽视的，由于 IT 系统先天的脆弱性，在保密性、完整性、可用性、可追溯性等方面存在的缺陷，势必给它的应用带来一些消极影响。

现如今，网络已深入到社会生活的方方面面，不仅在组织机构内严重依赖局域网，组织机构需要与各种外部单位发生联系，这主要使用的是互联网，因此保证信息的安全的需求，显得尤为重要。

1. 信息

ISO/IEC TR 13335《IT 安全管理指南》(简称 GMITS)中明确给出信息(Information)的定义："通过在数据上施加某些约定，然后给予这些数据特殊含义就是信息。"

常见的定义，信息指事物运动的状态和方式，是事物的属性，在增加了有关的约束条件后就会产生特殊的概念体系。实际中，知识、信号、情报、数据和消息通通理解为信息。信息从自身来看是无形的，在信息媒介的帮助下以多种形式存在或传播，它不仅可放在计算机、磁带、纸张等介质中存储，而且可以存放在人的大脑中，还可以利用网络、打印机、传真机等来传播。

从高校角度来看，信息可看作是资产的一种，不仅以计算机和网络中的数据形式存在，还以商业机密、专利、标准、管理规章、文件、图纸、关键人员等形式共存，与重要商业资产一样，信息资产同样拥有重要的价值，所以进行妥善保护是必要的。

2. 信息安全

从信息诞生以来，关于它的安全就备受人们的关注，不同的历史时期，技术上有所不同，因

而信息安全的工作重点、控制方式就会有一些差异。总体来看，信息安全大致经历了三个发展阶段。

(1)通信安全(COMSEC)

最早可追溯到20世纪初，当时的通信技术不太发达，只在传真、电报、电话等信息传输过程中存在安全问题。在当时的技术水平之下，人们关注的是信息的保密性，研究的是密码学，密码学成为当时最先进的安全技术，这一时期的信息安全可以概括为通信安全(Communication Security)，也可简称为COMSEC。

(2)信息安全

20世纪60年代，随着半导体、集成电路的快速发展极大地带动了计算机软硬件的发展，这一时期，计算机、网络的应用面越来越广，走入了实用化和规模化时期。这一时期对信息安全的要求是：对保密性、完整性和可用性有要求，即INFOSEC(Information Security)，这一时期美国、欧洲相继推出了可信计算机系统评价准则(简称TCSEC)和安全评价标准(简称ITSEC)。

(3)信息保障

20世纪80年代，由于互联网技术得到大发展，信息在局域网和广域网之间传输，这一时期的信息安全问题不受时间和空间的约束，信息安全关注的不再是传统的保密性、可用性和完整性三个原则，在当时的环境下，产生了真实性、抗抵赖性、可控性等原则和目标，信息安全演变成为：从全局角度考虑其体系建设的信息保障(Information Assurance)阶段，相关内容在美国的IATF(Information Assurance Technical Framework)规范中有明确阐述。

信息安全的概念是宽泛的、抽象的，身处在不同领域，对信息安全的解释会有所不同。现代信息系统是以互联网为基础建立的，信息安全有了确定的含义：保护信息系统中的所有硬件、有关软件和相关数据，让它们不再遭受不确定的、不怀好意的侵犯，使信息系统不再受到破坏、泄露、更改，让信息系统连续、可靠、正常地工作。对于经济领域而言，信息安全看重的是在缩减的同时控制风险，让业务操作平稳进行，同时将风险带来的不良影响尽可能地减少。

信息是资产的一种，同时也是各种行业正常业务往来、日常管理的重要资源。上升到国家层面，信息安全在国家安全中占有非常重要的战略地位。对一个单位而言，信息安全影响单位的正常运行和可持续发展；对于个人而言，保护个人隐私和财产安全，是信息安全责任所在。对于个人、组织、国家而言，确保重要的信息资产平安无事是至关重要的。信息安全的职责，就是要采取多种办法，可以是技术的、管理方式的变革，让信息资产发挥最大效能，换句话说就是将安全威胁减少，让一个单位实现正常运转。

所以说，可追溯性、保密性、可用性、真实性、完整性和可靠性等属于信息安全最关心的范畴，还是信息安全追求的目标。

3. 信息安全要素

说起信息安全，总是离不开所谓三元组的目标，就是众所周知的保密性、可用性和完整性，这就是信息安全的基本要素，同时也是安全建设所应遵循的根本原则。图2-1所示为信息安全三元组。

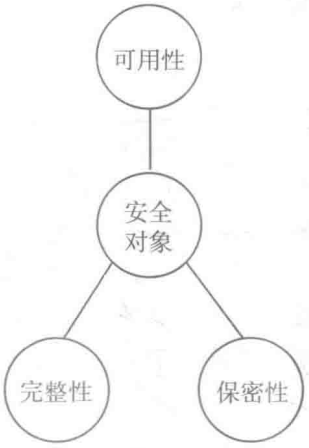

图 2-1　信息安全三元组

可用性(Availability)——实现拥有权利的客户、实体对信息、资源的合理访问，不至于被拒绝，允许及时有效地访问信息、资源。

完整性(Integrity)——保证信息在存储、使用、传输的时候不会被非法用户篡改，并且要禁止授权用户对系统、信息进行不适宜的篡改，让信息内、外部保持一致性。

保密性(Confidentiality)——保护信息在存储、使用、传输过程中不泄露给不合法客户或实体。

当然，不同机构和组织，因为需求不同，对 AIC 原则的侧重也会不同。如果组织最关心的是对私密信息的保护，就会特别强调保密性要求；如果组织最关心的是随时随地向客户提供正确的信息，那就会突出完整性和可用性的要求。

除了 AIC 三元组以外，信息安全还包含有其他原则，主要有可控性(Controllable)、真实性(Authenticity)、抗抵赖性(Non-repudiation)和可追溯性(Accountability)等，这些是对 AIC 三元组的进一步细化、增补或强化。

与 AIC 三元组相反的有一个 DAD 三元组的概念，即泄露(Disclosure)、篡改(Alteration)和破坏(Destruction)，实际上就是信息安全面临的最普遍的三类风险，是信息安全实践活动最终应该解决的问题。

信息安全的目标是保密性、完整性和可用性，或者再加上可控性、抗抵赖性等，但对 AIC 的追求只是一种简单抽象的理解，是信息安全的直接目标，而信息安全工作的最终目标还在于保证组织业务活动的连续性，AIC 目标是为追求业务连续性而服务的。

2.2　信息安全需求

在高校，信息是重要的资产之一，需要采取多种手段加以保护。在真正落实之前，高校务必清楚自己的安全需求，哪些信息资产需要保护，投入的力度有多大，应该达到什么样的保护