表 1 Rank 排序函数微课设计

微课基本信息	各个知识点	Rank 排序函数使用方法
	学科类型和教学对象	中职高一学生
	上课时间	8min
教学目标：引导学生掌握 Rank 排序函数的使用方法		
教学资源和环境：计算机、录屏软件以及 PPT		
教学过程： 第一，创设教学情境，引入主题； 第二，详细讲解 Rank 排序函数语法结构、功能以及参数说明； 第三，结合实际案例分析 Rank 排序函数的使用方法； 第四，总结课程内容，并布置相应的操作练习任务		
设计创新点： 本次教学中结合实际生活中的具体问题开展相应的教学互动，具有比较大的启发性以及趣味性，有助于提升学生学习过程中的主动性和积极性。微课视频便于学生反复观看，可以让本身接受能力不强的学生，同时也不好意思发问的学生可以反复观看、思考，有助于提升后进生的学习效果		

4.6.3 微课课程设计的实践应用

本次微课设计中，所采用的工具和软件主要为计算机、录屏软件以及 PPT，另外附带一个耳麦和话筒。具体的微课制作流程详情见表 2。

表 2 Rank 排序函数微课制作流程

步骤	内容
第一步	结合确定的教学内容，广泛收集和 Rank 排序函数相关的教学材料，其中也包括相关微练习题，以此实施 PPT 课件制作。
第二步	结合教学设计方案，初步制作完成录制脚本语言。
第三步	在计算机屏幕闪将视频录像软件以及教学 PPT 同时打开，带上耳麦对话筒位置以及音量结合实际需求调节，并对 PPT 界面以及录屏界面调整后，即可以实施录制。
第四步	完成录制后，美化教学视频，以便于使用

在现代互联网时代，我们日常生活中也出现了大量的微博、微信以及微电影等，成功进入到了“微时代”，大部分学生对于“微作品”也具有较大兴趣 [6]。所以在课堂教学中，微课的引入和应用，有助于提升学生的学习兴趣。同时在实际课程教学中，对于部分接受能力不高的学生，在学习过程中想要迅速掌握 Rank 排序函数的使用方法，难度较大，因此教学中将微课作为教学的辅助资源，引导这部分学生进行实例操作，进而提升这部分学生的实际操作能力。最后在课下，结合部分学生的学习需求，也能够将相关微课视频及配套资料上传到实训室服务器共享目录中去，便于学生自主下载学习，进而为学生自主学习、查漏补缺、巩固知识提供支持，以此产生触类旁通的学习效果。

在针对 Rank 排序函数使用方法微课设计教学尝试成功后，也可以将其他的重点函数作为知识点建构成系列化微视频，将其放置在同一个专题中，以便于学生系列化学习。经过实践研究发现，微课在中职计算机应用基础课程教学中的应用，可以显著提升学生的学习积极性和主动性，并提升教学质量。但是也需要注意到以下相关方面：第一，课程设计必须有效结合实际应用需求；微课课程中需要引入层次分明、趣味性强的总结；明确引导学生了解相应的学习方法，并实时给予必要的说明以及指导。第二，在掌握某个知识点的微课设计方法后，也需要掌握一个单元、一个学科的微课设计方法，必须建构系列化微课程，才能够在学生学习过程中为其提供系统化学习资源。比如在针对部分理论知识和实操重难点讲解中，可以将其制作成为微课，教学过程中适当地融入视频、动画以及音乐等多媒体素材，借助于生动有趣的教学资源，更加直观地将相关知识讲述给学生，提升学生的学习好奇心和就行，以此进一步提升课堂教学质量。第三，微课程设计中，不但要和学生实际情况和学习需求相结合，也必须注重为学生提供观察、观摩以及反思的空间，以此促进教师的专业化水平发展。

5 结语

综上，微课在中职“计算机应用基础”教学中的应用，对于教育教学工作的开展和创新具有重要促进作用。首先在微课的应用下，能够帮助学生确定具体的学习目标，微课可以结合中职学生学习能力和想要实现的学习目标，针对性地开展相应的教学活动，以此显著提升广大中职学生的学习能力。其次，微课的应用，也有助于丰富中职计算机应用基础课程内容。教师教学中，通过对微课的应用，实现对课程教学模式的优化，比如通过视频、PPT 等不同教学模式，以此实现对课程内容的丰富，提升课堂教学趣味性，在教学形式创新下提升学生学习兴趣，进而能够提升相应的课程教学质量。在微课特点的应用下，学生可以随时随地地结合自身需求开展相应的学习活动，提升学生自身学习能力，并培养学生终身学习理念，促进学生成长。最后，对于教师来讲，微课的有效应用，也有助于提升教学质量，降低教学难度，学生通过微课能够更好地去了解所学习的知识，充分掌握相应内容，进而显著提升自己的综合能力水平。

参考文献

[1] 林赛君.微项目式学习在中职计算机应用基础课程教学中的应用策略[J].开封文化艺术职业学院学报,2021,41(8):173-174.

[2] 张卉.浅议微项目学习在高职“计算机应用基础”课程教学中的应用[J].科学与信息化,2023(14):137-139.

[3] 任岳.微课在中职计算机应用基础课程教学中的应用探讨[J].科技资讯,2020,18(19):114-115+118.

[4] 李文丽,杨春燕.借助微课程优化并提升中职计算机应用基础教学效果的思路探索[J].卫生职业教育,2020,38(8):88-89.

[5] 仝磊.浅谈基于职业核心素养提升的中职计算机应用基础微课程体系建设[J].发明与创新・职业教育,2020(7):49+51.

[6] 韩晓.基于智慧课堂的中职《计算机基础》微课程的设计与实践[J].读与写,2020,17(31):18.

企业信息化建设中的网络安全管理问题研究

Research on Network Security Management Issues in Enterprise Informatization Construction

黄一航

Yihang Huang

重庆市合川区自来水有限责任公司　中国·重庆 401520

Chongqing Hechuan District Water Supply Co., Ltd., Chongqing, 401520, China

摘　要：论文旨在研究企业信息化建设中的网络安全管理问题，探讨信息化与网络安全之间的关系，并分析企业信息化建设中所面临的网络安全问题。同时，阐述了网络安全管理模型和框架，包括安全政策和标准制定、风险评估和管理、安全培训和教育、安全监控和事件响应以及合规性和法规遵从。针对问题，提出企业信息化建设中的网络安全最佳实践，包括安全策略和规程的制定、员工培训和教育、安全技术的应用、风险管理和响应策略以及安全文化的建立，以帮助企业更好地应对网络安全挑战。

Abstract: The purpose of this paper is to study the network security management problems in enterprise informatization construction, discuss the relationship between informatization and network security, and analyze the network security problems faced in enterprise informatization construction. At the same time, the cybersecurity management model and framework are elaborated, including security policy and standard development, risk assessment and management, security training and education, security monitoring and incident response, and compliance and regulatory compliance. In view of the problems, the best practices of network security in enterprise informatization construction are proposed, including the formulation of security policies and procedures, employee training and education, the application of security technology, risk management and response strategies, and the establishment of security culture, so as to help enterprises better cope with network security challenges.

关键词：信息化建设；网络安全；安全管理

Keywords: informatization construction; network security; security management

DOI: 10.12346/csai.v2i1.9113

1 引言

随着信息化技术的飞速发展，企业信息化建设已成为提高竞争力和效率的关键要素。然而，信息化建设也带来了网络安全问题的增加，这些问题可能对企业的机密性、完整性和可用性产生严重影响。因此，企业需要采取有效的网络安全管理措施来应对这些挑战。

2 信息化建设和网络安全的关系

2.1 信息化建设依赖于网络基础设施

信息化建设是现代企业通过广泛应用互联网、局域网和云计算等网络技术，企业能够实现数据共享、远程办公、实时协作等多种功能。这种数字化转型不仅提高了企业的效率和竞争力，还为企业开创了更多商机。然而，值得注意的是，这一切都依赖于网络基础设施的高可用性和可靠性。网络是信息化建设的支撑，是数据流动的媒介，如果网络存在漏洞或受到网络攻击威胁，信息化建设将陷入困境。网络的稳定性和安全性对企业来说至关重要，因为它们直接关系到业务的持续性和可靠性。如果网络遭受严重的攻击或故障，企业可能会经历业务中断，导致重大损失，同时也可能泄漏敏感信息，造成声誉损害和法律问题。因此，信息化建设的成功

【作者简介】黄一航（1991-），男，中国重庆人，本科，工程师，从事网络信息化、智慧水务研究。

与否密切关联着网络基础设施的安全性和可用性 [1]。

2.2 信息化建设增加了网络安全的复杂性

企业在信息化建设过程中不可避免地涉及大量的敏感数据，包括客户个人信息、财务数据、研发成果等，这些数据在数字化转型中通过网络传输和存储。虽然数字化带来了数据的高效利用，但也将数据置于网络安全的焦点之下。信息化建设增加了网络安全的复杂性，因为企业必须同时考虑数据的保密性、完整性和可用性。数据的泄露、篡改或丢失可能对企业造成严重损害，因此，网络安全措施必须足够复杂和全面，以应对各种潜在的威胁。此外，不同部门和业务领域可能需要不同级别的网络安全保护，这增加了网络安全策略的多样性和挑战。因此，信息化建设不仅提高了网络安全的复杂性，还需要企业采取更多技术和策略来确保数据和网络的安全性。

2.3 信息化建设提高了网络攻击的威胁

随着企业信息化建设的普及，黑客和恶意攻击者也寻求新的机会入侵企业网络。企业广泛使用的应用程序、软件和云服务可能存在漏洞，这些漏洞成为黑客攻击的入口。此外，黑客采用了更加精密和隐秘的攻击技术，如钓鱼攻击、勒索软件、零日漏洞利用等，这使得网络攻击更加难以防范和发现。信息化建设提高了网络攻击的威胁多样性，从传统的病毒和恶意软件到更高级的网络入侵和社交工程攻击。企业必须不断升级其网络安全策略，以应对不断演化的威胁，这也增加了网络安全的挑战。因此，信息化建设虽然带来了商业机会，但也提高了网络安全威胁的复杂性和难度，企业必须保持警惕，采取积极的网络安全措施来保护其数字资产和业务 [2]。

3 企业信息化建设中的网络安全面临的问题

3.1 数据泄露

数据泄露是企业信息化建设中最常见和严重的网络安全问题之一。企业在信息化建设中处理大量敏感数据，包括客户信息、财务数据和知识产权等，这些数据可能受到黑客攻击、内部泄露或无意间的数据外泄威胁 [2]。数据泄露可能导致严重的后果，包括客户信任的损失、法律诉讼和财务损失。为应对这一问题，企业需要采取数据分类、加密、访问控制和监控等措施，确保敏感数据的保护，同时建立灵活的应急响应计划以迅速应对潜在的数据泄露事件。

3.2 网络入侵

网络入侵是指黑客或恶意攻击者成功越过企业网络的防御系统，获取未经授权的访问权或控制。这可能导致数据盗窃、业务中断和系统破坏等问题。企业需要不断提升网络安全，包括防火墙、入侵检测系统、安全漏洞管理和多因素身份验证等措施，以减少入侵的风险。此外，实时监控和事件响应计划也是关键，以便快速检测和应对入侵事件 [3]。

3.3 恶意软件

恶意软件是一种网络安全问题，包括病毒、勒索软件和木马程序等。这些恶意软件可以感染企业的系统，导致数据损坏、勒索或非法访问。防范恶意软件攻击的关键措施包括使用强大的防病毒软件、定期更新和升级操作系统和应用程序、教育员工如何辨识恶意软件，并备份数据以防止数据丢失。

3.4 社交工程攻击

社交工程是攻击者通过欺骗和操纵技巧来获取敏感信息或访问权限的手段。攻击者可能通过伪装成可信任的实体或通过欺骗员工来获取访问凭据或敏感数据。为防止社交工程攻击，企业需要加强员工的安全培训和教育，增强他们的风险意识，教导他们如何警惕可疑请求以及如何安全地处理敏感信息。同时，企业也应该实施强有力的身份验证措施，以确保只有合法用户能够访问敏感信息。

4 网络安全管理模型和框架

4.1 安全政策和标准制定

首先，安全政策的制定需要考虑到企业所处的行业特点。不同行业面临的网络威胁和合规性要求可能各不相同。例如，金融行业需要特别关注支付交易的安全性和合规性，而医疗行业则需重点考虑病患隐私数据的保护。因此，在制定安全政策时，必须充分了解行业标准和最佳实践，确保政策能够满足行业特定的要求 [4]。

其次，安全政策和标准需要以高深的计算机语言和技术术语来表达，以确保准确性和清晰度。例如，对于访问控制政策，需要明确定义角色和权限，使用精确的术语来描述不同层次的访问权限。此外，密码策略需要包括复杂性要求、定期更改密码的规定以及多因素身份验证的具体实施细节。这些技术性细节是安全政策和标准的核心，确保了企业网络的防护措施得以有效执行。

最后，安全政策和标准的制定还需要考虑到未来的网络安全威胁和技术演进。网络安全领域不断发展，新的威胁和攻击技术不断涌现 [3]。因此，安全政策和标准必须具备灵活性，能够根据不断变化的威胁环境进行更新和调整。这包括定期的审查和评估，以确保政策和标准仍然适用于新的网络安全挑战。

4.2 风险评估和管理

风险评估和管理在企业网络安全中扮演着关键的角色。它需要企业先识别和评估潜在的网络安全风险，这包括系统漏洞、恶意软件、外部和内部威胁等各方面的考量。这一过程涉及多种方法和技术，包括数学建模、漏洞扫描和弱点分析等。通过数学模型和方程的应用，企业可以量化潜在威胁的概率和影响，以更准确地评估风险的严重程度。一旦风险被明确定义和评估，接下来的步骤是采取措施来管理这些风险。风险管理策略可以包括风险缓解、风险转移、风险接受或风险规避等不同的方法。计算机语言和数学方程的应用可以帮助企业优先处理高风险威胁，从而降低潜在的损失 [4]。

例如，成本—效益分析可以用来比较不同的安全投资，以确定哪种策略对降低风险最为经济高效。

此外，风险管理还包括建立数学模型和方程，以评估不同风险管理策略的效益。这可以帮助企业决策哪种策略最适合其具体情况以及如何最大程度地减少网络威胁对企业的影响。

4.3 安全培训和教育

安全培训和教育是确保员工对网络安全问题有足够的认识和技能的关键组成部分。员工往往是企业网络安全的第一道防线，因此他们需要了解网络威胁、如何辨识可疑活动以及如何安全地处理敏感信息。培训还应涵盖对安全政策和标准的理解和遵守。通过定期的培训和教育，员工可以增强网络安全意识，减少人为失误和社交工程攻击的风险，从而加强整体网络安全。

4.4 安全监控和事件响应

了解您的要求，您希望将关于安全监控和事件响应的内容与数学方程和计算机语言结合在一起，以创建一个段落。下面是满足您要求的段落：

安全监控和事件响应在企业网络安全中扮演着至关重要的角色。这些关键环节不仅需要高效的监控系统，以实时监测网络活动和检测潜在的威胁，还需要利用数学方程和计算机语言来提高精确性和速度。

风险评估方程是其中之一，通过以下方程计算特定风险的量化值：

$$Risk = Threat \times Vulnerability \times AssetValue$$

这个方程帮助企业确定事件的风险级别，有助于确定事件的优先级和响应策略。同时，事件严重性评估方程结合以下方式来评估事件的严重性：

$$Severity = Likelihood \times Impact$$

通过计算事件的严重性，可以更好地确定事件的重要性和响应优先级。

攻击风险评估方程帮助企业量化特定攻击的风险，考虑了多个因素，如威胁来源、漏洞利用可能性、攻击的影响等。最后，事件响应时间方程允许企业估算事件响应所需的时间，涵盖了各个阶段，包括检测、分析、隔离、根除和恢复。结合计算机语言的自动化能力，有助于企业更准确地发现、分析和应对安全事件。这种综合方法提高了网络安全的效率和准确性，降低了潜在的损失和风险。它是确保业务连续性和网络的可持续性的不可或缺的一部分。

4.5 合规性和法规遵从

网络安全管理中，合规性和法规遵从是不可忽视的要素。企业必须遵守适用的法律法规和行业标准，以保护客户数据和敏感信息，同时避免潜在的法律责任。这包括隐私法、数据保护法、金融合规性要求等各种法规。建立合规性框架，确保网络安全措施符合法律要求，同时进行定期的合规性审查和报告，以确保企业网络安全一直保持在合规状态下。

5 企业信息化建设中的网络安全最佳实践

网络安全在今天的数字时代变得至关重要。随着企业信息化建设的不断推进，企业依赖于网络和数字技术来支持业务运营、数据存储和交流。然而，随之而来的是网络威胁和风险的不断增加。黑客、病毒、勒索软件和数据泄露等威胁不断演化，对企业的网络安全构成了严峻挑战。

5.1 安全策略和规程的制定

在企业信息化建设中，安全策略和规程的制定是确保网络安全的基石。安全策略是企业网络安全的指导原则，它明确了安全的目标、原则和要求。通过数学模型，可以评估不同策略对网络安全的影响。例如，通过成本—效益分析，可以确定哪种策略最具经济性。此外，计算机语言可以用于自动化策略执行，确保安全控制的一致性。通过制定清晰的安全规程，如对敏感数据的访问控制、密码策略和网络使用规定，企业可以确保员工了解并遵守安全要求 [5]。安全策略和规程的制定不仅有助于降低风险，还能提高网络安全的可维护性和可管理性，确保业务的连续性。

5.2 安全技术的应用

在网络安全最佳实践中，安全技术的应用是关键环节。企业应该选择适合其需求的安全技术，并将其整合到信息化建设中。数学模型和计算机语言在这方面可以发挥巨大的作用。例如，使用数学模型来评估不同安全技术的效果，帮助企业选择最适合的技术。计算机语言可以用于开发自定义的安全工具和应用程序，以满足特定的安全需求。此外，数学模型还可以用于评估安全技术的性能。例如，通过模拟攻击和防御场景来测试安全系统的鲁棒性。安全技术的应用不仅有助于防止潜在的威胁，还提高了网络的弹性和适应性，使企业能够更好地抵御新兴的网络攻击。

5.3 风险管理和响应策略

风险管理和响应策略是信息化建设中的另一个关键方面。通过数学模型，企业可以识别和评估潜在的网络安全风险，以确定哪些威胁对其最为关键。风险管理的目标是降低网络安全威胁对企业的影响，确保业务的连续性和稳定性。计算机语言在风险响应方面可以用于自动化响应措施。例如，根据风险评估自动调整安全策略。此外，数学模型还可以用于评估不同风险管理策略的效益，帮助企业决策哪种策略最适合其具体情况。

5.4 安全文化的建立

安全文化的建立是信息化建设中的关键要素。企业需要将安全意识融入组织的 DNA 中，使每个员工都成为网络安全的守护者。数学模型可以用于评估安全文化的健康程度，通过员工的安全行为数据来测量安全文化的改进。计算机语言可以用于开发安全培训和教育工具，以增强员工的网络安全意识。通过建立积极的安全文化，企业可以降低内部威胁的风险，增强整体的网络安全。